



User Manual

DAG1000-4s

☎ +86 755 61919966

🌐 www.dinstar.com

✉ support@dinstar.com

Preface

Welcome

Thanks for choosing the **DAG1000_4S VoIP Gateway**! We hope you will make full use of this rich-feature FXS VoIP Gateway. Contact us if you need any technical support: +86-755-61919966.

About This Manual

This manual provides information about the introduction of the analog VoIP gateway, and about how to install, configure or use it. Please read this document carefully before install the gateway.

Intended Audience

This manual is aimed primarily at the following people:

- Users
- Engineers who install, configure and maintain the gateway.

Contents

1 Product Introduction.....	1
1.1 Overview	1
1.2 Application Scenario.....	1
1.4 Description of Interfaces and Indicators.....	2
1.5 Functions and Features.....	3
1.5.1 Key Features	3
1.5.2 Physical Interface	3
1.5.3 Voice & FAX	3
1.5.4 Supplement Service	4
1.5.5 FXS.....	4
1.5.6 Software Features	4
1.5.7 Maintenance	5
1.5.8 VOIP	5
1.5.9 Security	6
1.5.10 Environmental	6
2 Quick Installation.....	8
2.1 Installation Attentions	8
2.2 Installation Steps	8
3 Basic Operations	10
3.1 Methods to Number Dialing.....	10
3.2 Direct IP Calls.....	10
3.3 Call Holding	11
3.4 Call Waiting	11
3.5 Call Transfer	11
3.5.1 Blind Transfer	11
3.5.2 Attended Transfer.....	11
3.6 Three-way Calling.....	12
3.7 Description of Feature Codes.....	12
3.8 Sending and Receiving Fax.....	14
3.8.1 T. 38 and Pass-Through.....	14
2.9 Local IVR Operation	14
2.9.1 Inquire IP address	14
2.9.2 Factory Reset	14
2.9.3 Configure LAN Port's IP Address	15
4 Configurations on Web Interface.....	16
4.1 Network Connection	16

4.2	Preparations for Login	16
4.3	Log in Web Interface	17
4.4	Navigation Tree	18
4.5	State and Statistics.....	19
4.5.1	System Information.....	19
4.5.2	Port Status.....	21
4.5.3	Current Call	22
4.5.4	RTP Session.....	22
4.5.5	CDR.....	22
4.5.6	Record Statistics	23
4.5.7	VPN State.....	23
4.6	Quick Setup Wizard.....	24
4.7	Network Configuration	24
4.7.1	Local Network.....	24
4.7.2	VLAN (Virtual Local Area Network).....	27
4.7.3	DHCP Option.....	28
4.7.4	QoS	29
4.7.5	DHCP Server (Route Mode)	29
4.7.6	DMZ Host (Route Mode).....	30
4.7.7	Forward Rule (Route Mode).....	30
4.7.8	Static Route (Route Mode).....	31
4.7.9	Firewall-Forward Rule (Route Mode).....	32
4.7.10	ARP	33
4.7.11	VPN	33
4.8	SIP Server	35
4.9	IP Profile.....	38
4.10	Tel Profile	40
4.11	Port.....	41
4.12	Advanced	44
4.12.1	Line Parameter	44
4.12.2	FXS Parameters	46
4.12.3	Media Parameter	47
4.12.4	Service Parameter.....	49
4.12.5	SIP Compatibility	53
4.12.6	NAT Parameter	58
4.12.7	Speed Dial	59
4.12.8	Feature Codes.....	60
4.12.9	System Parameter.....	63
4.13	Call & Routing.....	66
4.13.1	Wildcard Group.....	66
4.13.2	Port Group	67
4.13.3	IP Trunk.....	69

4.13.4	Routing Parameter	70
4.13.5	IP -> Tel Routing	71
4.13.6	Tel->IP/Tel Routing	71
4.14	Manipulation	72
4.14.1	IP -> Tel Called.....	72
4.14.2	Tel -> IP/Tel Caller.....	74
4.14.3	Tel-IP/Tel Called	75
4.15	Routing rule examples.....	77
4.15.1	Route any calls from any IP to specific port	77
4.15.2	Route any calls from any IP to specified port group	77
4.15.3	Route any calls from any port to specific SIP IP trunk	78
4.16	Maintenance.....	79
4.16.1	TR069.....	79
4.16.2	SNMP	81
4.16.3	Syslog.....	84
4.16.4	Provision.....	84
4.16.5	User Manage	85
4.16.6	Radius Parameter	86
4.16.7	Action URL	86
4.16.8	SIP PNP	87
4.16.9	NMS.....	88
4.16.10	TACACS Parameter	88
4.16.11	WEB Log.....	89
4.17	Security	89
4.17.1	WEB ACL	89
4.17.2	Telnet ACL.....	90
4.17.3	Device ACL	90
4.17.4	Firewall-Input Rule	91
4.17.5	Passwords.....	94
4.17.6	Encrypt	95
4.17.7	Certificate Manage	95
4.18	Tools.....	97
4.18.1	Firmware upload.....	97
4.18.2	Data Backup	98
4.18.3	Data Restore	98
4.18.4	Outward Test.....	98
4.18.5	Ping Test	99
4.18.6	Tracert Test	100
4.18.7	Network Capture.....	101
4.18.8	Factory Reset	103
4.18.9	Device Restart.....	103
5	Trouble Shooting	104

6 Glossary.....	106
------------------------	------------

1 Product Introduction

1.1 Overview

DAG1000_4S VoIP gateway provides voice services based on IP network. It's a cost-effective and flexible solution for SOHO (Small Office-Home office), remote office, medium-sized enterprise and enterprise with multiple branches.

The gateway connects to analog telephone, fax and traditional analog PBX with standard voice interfaces and provides high quality voice service.

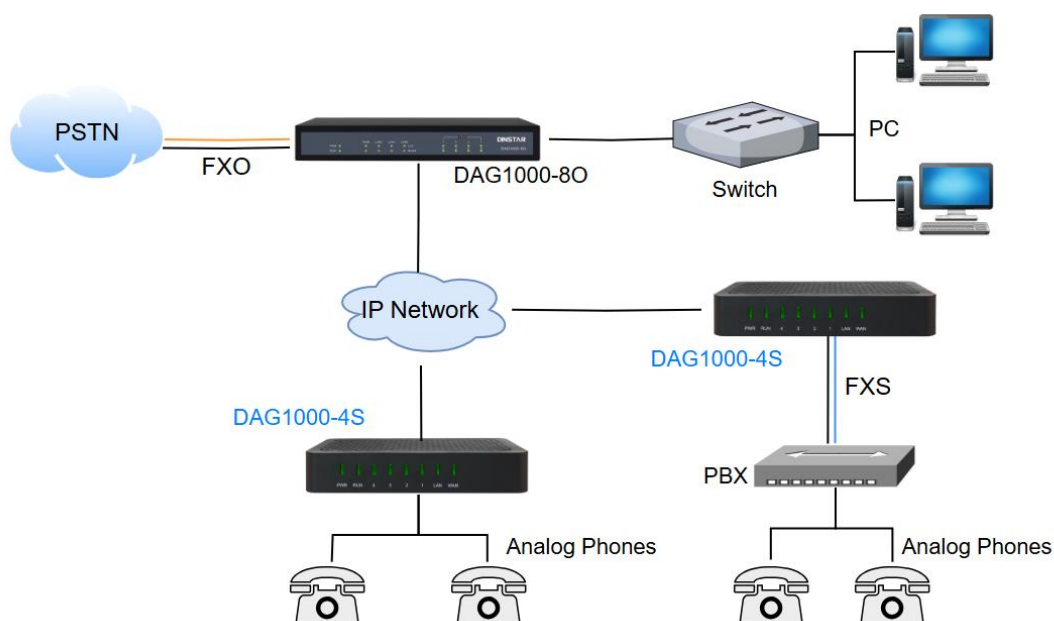
The gateway, based on standard SIP protocol is compatible with leading IP PBX, soft-switch and SIP-based platform.

The FXS analog gateway available in the following configurations:

Model	Voice Channels	FXS Ports	Physical Port Labels
DAG1000-4S	4	4	1-4

For detailed hardware and software features, please refer to “product specifications”.

1.2 Application Scenario



1.3 Equipment Appearance

① DAG1000-4S



Front View



Back View

1.4 Description of Interfaces and Indicators

NO	Port and Indicator	Color	Status	Description
1	Power Indicator	Green	Off	The gateway is powered on
			On	The gateway is powered off or there is no power supply
2	Running Indicator (Alarm Status)	Green	Slow Flashing	Slow flashing with 1s On, 1s OFF means the gateway is running properly
			Fast Flashing	Fast flashing with 0.25s ON, 0.25s OFF means there is a SIP account registered successfully
			On/Off	Continuously ON or OFF, means gateway is Alarm status or running improperly.
3	FXS Indicator	Green	On	FXS port is currently occupied by a call
			Off	FXS port is idle or faulty
4	WAN/LAN Indicator	Green	Green Flashing	The gateway is properly connected to network
			Off	The gateway is not connected to network or network connection is improper way

5	FXS Port	N/A	N/A	FXS ports to connect standard analog phone or FAX machine or a PBX
6	Network Port	N/A	N/A	To connect to the IP network over a DSL modem or Router or a LAN switch
7	RST Button	N/A	N/A	To restore factory settings (please use with caution)
8	Power Jack	N/A	N/A	To connect DC 12V power supply

1.5 Functions and Features

1.5.1 Key Features

- Fax over IP (T.38 and Pass-Through)
- Support IPv4 and IPv6
- TR069 and SNMP
- Multiple codecs: G.711A/U, G.723.1, G.729A/B, iLBC, AMR
- Fully compatible with leading IMS/NGN, SIP based IP telephony system

1.5.2 Physical Interface

- Capacity

4 FXS, RJ11

- Ethernet Interface

1*WAN, 10/100Mbps, RJ-45

1*LAN, 10/100Mbps, RJ-45

1.5.3 Voice & FAX

- G.711A/U law, G.723.1, G.729A/B, G.726, AMR, iLBC, AMR
- Silence Suppression
- Comfort Noise Generation (CNG)
- Voice Activity Detection (VAD)
- Echo Cancellation (G.168), with up to 128ms
- Adaptive (Dynamic) Jitter Buffer
- Hook Flash
- Programmable Gain Control

- T.38/Pass-through
- High speed fax up to 14.4kbps
- Modem/POS
- DTMF mode: Signal/RFC2833/INBAND
- VLAN 802.1P/802.1Q (Voice/data/management VLANs)
- Layer3 QoS and DiffServ

1.5.4 Supplement Service

- Call Waiting
- Blind Transfer
- Attend Transfer
- Call Forward on Busy
- Call Forward on No Reply
- Unconditional Call Forward
- Warm/Immediately Hotline
- Call Hold
- Do-not-disturb
- 3-Way Conference
- Message Waiting Indicator
- Speed Dial

1.5.5 FXS

- Connector: RJ11
- Dial Mode: DTMF and Pulse
- Pulse: 10 and 20 PPS
- Caller ID: DTMF/FSK CLI Presentation
- Max Cable Length: 3KM
- Reversed Polarity
- Programmable Call Progress Tone

1.5.6 Software Features

- Hunting Group

- Web ACL
- Telnet ACL
- Action URL
- PPPoE/IPv4/IPv6
- OpenVPN
- Digitmap
- Routing Rules based Prefixes
- Caller/Called Number Manipulation

1.5.7 Maintenance

- SNMP v1/v2/v3
- TR069, TR181
- Auto Provisioning
- Web/Telnet
- Configuration Backup/Restore
- Firmware Upgrade via Web
- CDR
- Syslog (Emerg, alert, critical, error warning, notice, info, debug)
- Ping/Tracert Test
- Network Capture
- Outward Test (GR909)
- NTP/Daylight Saving Time
- IVR local Maintenance
- Cloud-based Management

1.5.8 VOIP

- SIP V2.0 (UDP/TCP), RFC 3261,3262,3263,3264,3265
- RFC 3515, RFC2976, RFC3311, RFC3891, RFC3892, RFC3489
- ETC (3GPP TS24.629)
- SDP (RFC 2327)
- RTP/ SRTP/RTCP (RFC 2833,2198,1889)

- SIP over TLS
- RFC4028 Session Timer
- RFC3266 IPv6 in SDP
- RFC2806 TEL URI
- RFC3581 NAT, rport
- Primary/backup SIP server
- Outbound Proxy
- DNS SRV/ A Query/NATPR Query
- SIP Trunk
- Early Media/Early Answer
- NAT: STUN, Static/Dynamic NAT

1.5.9 Security

- Firewall
- Prevention DDoS attacks
- Control of Access Policies
- MAC spoofing protection
- DHCP flood protection
- Stateful inspection (SPI)
- Packet filtering
- Access Rule List
- Certificate management / Encryption settings
- Password Complexity Requirement

1.5.10 Environmental

- Power Supply:100-240VAC, 50-60 Hz@DC12V 1A
- Power Consumption: 5W(Typical)
- Operating Temperature:0 °C~ 45 °C
- Storage Temperature: -20 °C~80 °C
- Humidity:10%-90% Non-Condensing
- Dimensions(W/D/H): 140*86*25mm

- Unit Weight: 0.3kg

2 Quick Installation

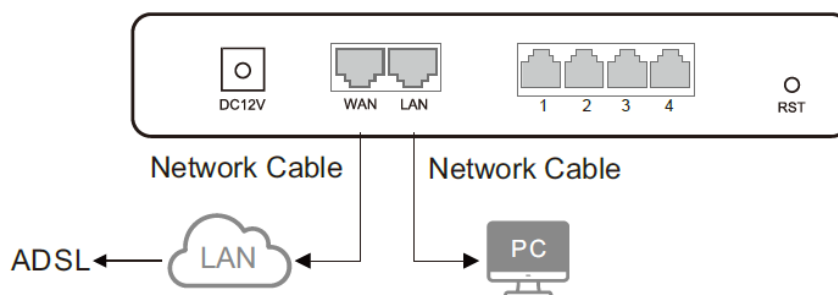
2.1 Installation Attentions

To avoid unexpected accident or device damage, please read the following instructions before installing the DAG1000-4S device:

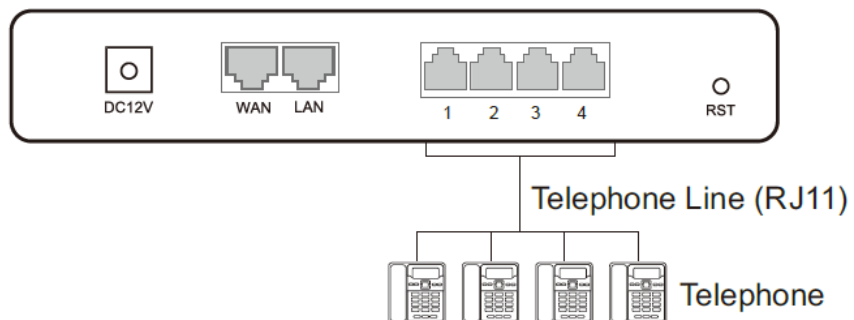
- Anti-jamming: to reduce the interference with telephone calls, it's highly recommended that telephone lines connected to the gateway should be placed away from power cables.
- Power supply: the power adapter of the gateway accepts Dc input voltage of 12V. Please ensure safe and stable power supply.
- Network bandwidth: please ensure there is enough network bandwidth so as to guarantee stabilized running of the gateway.
- Temperature and humidity: to avoid any accident that might cause malfunction, it's advised to install the gateway in an equipment room where temperature and humidity are appropriate.
- Ventilation: to avoid overheating, please do not pile up the gateway with other devices and make sure the gateway has good ventilation around.
- Mechanical load: please make sure the gateway is placed steadily to avoid damage. It's highly advised to horizontally place the gateway on a flat surface or a cabinet.

2.2 Installation Steps

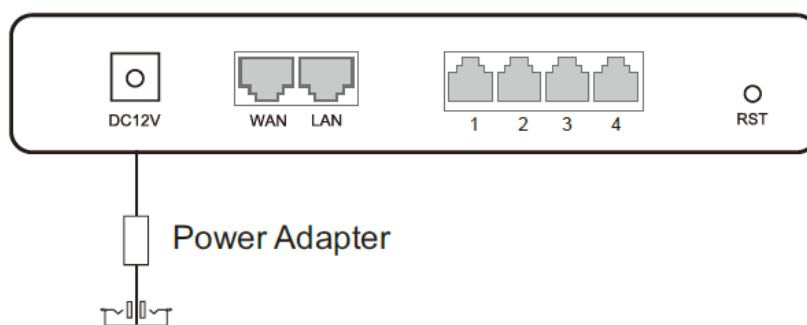
► Network Connection



► Telephone Connection



► Power Connection



3 Basic Operations

3.1 Methods to Number Dialing

Dial mobile phone or extension number

- Dial the number directly and wait for 3 seconds (Default “No dial timeout”);
- Dial the number directly and press #.

3.2 Direct IP Calls

The gateway allows users to directly call through IP address. Under this circumstance, the user only needs an analog phone which is connected to a FXS port of the gateway, and calls can be established without register.

Calls can be established through IP address as long as one of the following conditions is met.

- Both the gateway and other VoIP device have public IP addresses;
- The gateway and other VoIP device use private IP addresses of a same LAN;
- The gateway and other VoIP device can be connected through a router and use public or private IP addresses (with necessary port forwarding or DMZ).

Operation Process:

Step1: Pick up the analog phone and then dial “*47”;

Step2: Enter the target IP address.

Note:

No dial tone will be played between step 1 and step 2

Example:

Assume that the target IP address is 192.168.0.160, user need to dial *47 and then **192*168*0*160**. After that, press the “#” key or wait 3 seconds. Then signaling interaction is completed and ringing can be heard.

Note:

You cannot make direct IP calls between FXS0 to FXS1 of a same DAG1000-4S since they are using same IP addresses. Call through IP address is only routed to the default destination port 5060.

3.3 Call Holding

Place a call on hold by pressing the “flash” button on the analog phone (if the phone has the button). Press the “flash” button again to release the previously held caller and resume conversation. If no “flash” button is available, use “hook flash” instead.

3.4 Call Waiting

If a calling party places a call to a called party which is otherwise engaged, and the called party has the call waiting feature enabled, the calling party will hear a IVR voice ‘Please hold on, the subscriber you dialed is busy’ and the called party will hear three beeps.

By pressing the flash button or the flash hook, the called party is able to switch between the new incoming call and the current call.

3.5 Call Transfer

3.5.1 Blind Transfer

Blind transfer is used to transfer call to a third party without informing the caller. Assume that A and B are in a conversation. A wants to blind Transfer B to C:

- A presses **Flash** on the analog phone to hear the dial tone;
- Then A dials ***87** and C’s number and # (or wait for 4 seconds);
- A will hear the confirm tone. Then, A hangs up, and B and C enter into a conversation.

Note:

“Call features enable” must be set to “Yes” on WEB configuration page. Caller A can place a call on hold and wait for one of the three situations:

- A quick confirmation tone (similar to call waiting tone) which follows the dial tone. This indicates the transfer is successful. At this point, Caller A can either hand up or make another call.
- A quick busy tone which follows a restored call (on supported platforms only). This means the transferee has received a 4xx response for the INVITE and we will try to recover the call. The busy tone indicates the transfer has failed.
- Continuous busy tone. This means the call has timed out.

3.5.2 Attended Transfer

Attended transfer allows the transferring party either connects the call to a ringing phone (ringbackheard) or speaks with the third party before transferring the call to the third party.

Assume that A and B are in conversation. Caller A wants to *attended transfer* B to C:

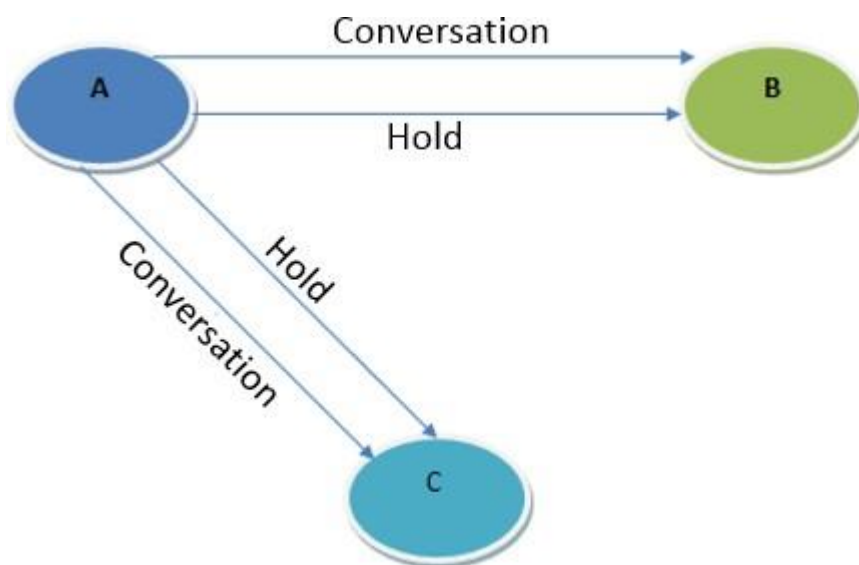
- A presses Flash on the analog phone and wait for dial tone;

- Then dial C's number followed by # (or wait for 3 seconds);
- If C answers the call, A and C are in conversation. Then A can hang up to complete the transfer;
- If C does not answer the call, A can press "flash" to resume call with B.

3.6 Three-way Calling

Three-way calling:

- A calls B, B picks up the phone, then A and B enters into conversation;
- A presses the hook flash, and the call between A and B is placed on hold. Then C calls A and A answers the call.
- A presses hook flash again, then the calls between A and B and between A and C are placed on hold. At this time, if A presses 1 , conversation between A and B is resumed; if A presses 2, conversation between A and C is resumed; if A presses 3, A,B and C enter into conversation.



3.7 Description of Feature Codes

The gateway supports all traditional and senior phone function. It provides feature codes for easy maintenance and easy entry to phone functions.

Feature Codes	Corresponding Function
*158#	Dial *158# to inquiry the IP address of LAN port
*159#	Dial *159# to inquiry the IP address of WAN port

*114#	Dial *114# to inquire port account
*115#	Dial *115# to query the phone number of a FXS port group
*168#	Dial *168# to query the register status of a FXS port
*154#	Dial *154# to remove login limit
150	Dial *150* to set the way of obtaining IP address
157	Dial *157*0 to set route mode; dial *157*1 to set bride mode
152	Dial *152* to set IPv4 address
153	Dial *153* to set subnet mask
156	Dial *156* to set default gateway's IP address
*170#	Dial *170# to increase the sound volume of a FXS port
*171#	Dial *171# to decrease the sound volume of a FXS port
160	Dial *160*?# to enable or disable web or telnet access via the WAN or LAN port in router mode.
165	Dial *165*000000# to restore username/password and network configuration to factory defaults
166	Dial *166*000000# to reset to factory defaults
*111#	Dial *111# to restart the gateway
47	Dial *47* to establish a call through IP address
*51#	Dial *51# to enable 'call waiting' feature
*50#	Dial *50# to disable 'call waiting' feature
87	Dial *87* to blind transfer a call
72	Dial *72* to enable 'unconditional call forwarding' feature
*73#	Dial *73# to disable 'unconditional call forward' feature
90	Dial *90* to enable 'busy call forwarding' feature
*91#	Dial *91# to disable 'busy call forwarding' feature
92	Dial *92* to enable 'no answer call forwarding' feature
*93#	Dial *93# to disable 'no answer call forwarding' feature
*78#	Dial *78# to enable DND
*79#	Dial *79# to disable DND

*200#	Dial *200# to access voice mail
*#	Dial *# to place a call on hold
##	When the port has two calls, if dial ##, release the current call and restore the inactive call.
Flash/Hook	Used to switch between incoming calls. If the phone is not in session, flash/hook will switch a new channel for a new call.

3.8 Sending and Receiving Fax

The gateway supports four fax modes:

- T.38 (FoIP)
- Pass-Through
- Modem
- Adaptive

3.8.1 T. 38 and Pass-Through

T.38 is the preferred fax mode because it is more reliable and works well in most network conditions. If the service provider supports T.38, please use this method by selecting T.38 as fax mode (default). If the service provider does not support T.38, pass-through mode may be used. If you have problems with sending or receiving Fax, toggle the Fax Tone Detection Mode setting.

2.9 Local IVR Operation

2.9.1 Inquire IP address

Connect analog phone to FXS ports of the DAG1000-4S gateway, then pick up the phone. After dialing tone, dial *158# to inquire the IP address of LAN port and dial *159# to inquire the IP address of WAN port.

2.9.2 Factory Reset

Pick up the phone, and then dial *166*000000#. After hearing a voice prompt of 'setting successfully', hang up the phone and the gateway is reset to factory defaults.

2.9.3 Configure LAN Port's IP Address

Before configuration, please ensure:

- The gateway is power on;
- Device has been connected to network;
- Telephone is connected to FXS port of the gateway.

Configure dynamic IP address by DHCP:

Pick up the phone, dial *150*2# and then hang up the phone.

If the voice prompt indicates 'setting successfully', please restart the gateway after 10 seconds.

Configure Static IP address:

Take the configuration of IP address '172.16.0.100' as example.

Pick up the phone, dial *150*1# and then hang up the phone.

Then configure IP address and mask as follow:

- Configure IP address

Pick up the phone, dial *152*172*16*0*100# and then hang up the phone.

- Configure subnet mask

Pick up the phone, dial *153*255*255*0*0# and then hang up the phone.

- Configure gateway IP address

Pick up the phone, dial *156*172*16*0*1# and then hang up the phone.

Query the IP address of the gateway: Pick up the phone, dial *158#.

If the gateway uses PPPoE method to get IP address, the IP address needs to be configured through web browser.

Note:

The telephone will play voice prompt "setting successfully" if the step is correct.

4 Configurations on Web Interface

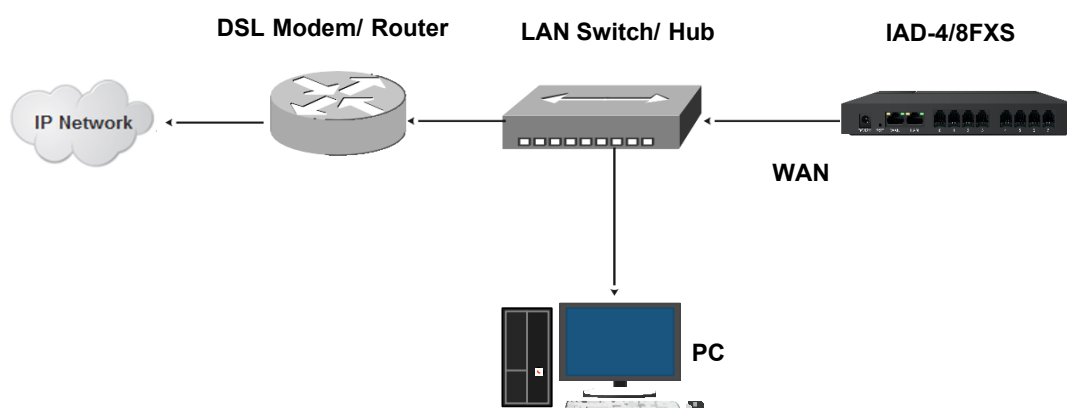
4.1 Network Connection

DAG1000-4S works in two modes: route mode and bridge mode. When it is under the route mode, the IP of WAN port must be different from the IP of LAN port. But when it is under the bridge mode, the IP of WAN and the IP of LAN are the same.

Under the route mode, the default IP address of WAN port is a DHCP IP address, while the default IP address of the LAN port is 192.168.100.1.

Under the bridge mode, both the default IP addresses of the WAN port and the LAN port are 192.168.100.1.

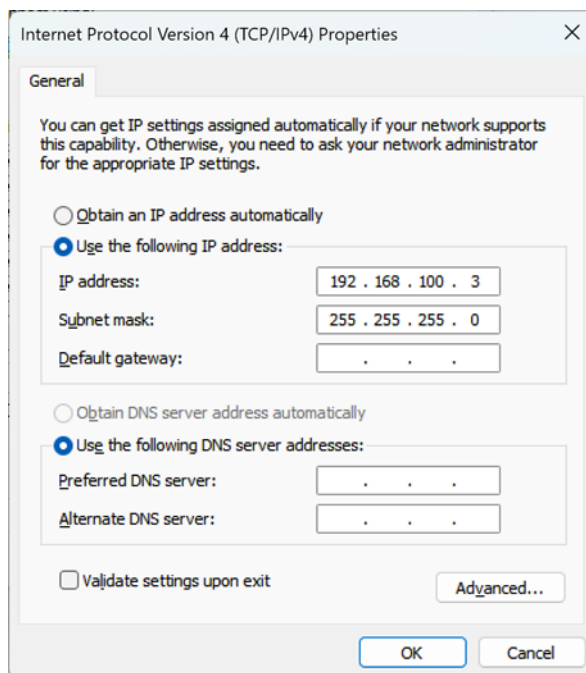
Connect the DAG1000-4S gateway to the network according to the following network topology, and dial *158 to query the IP address of the gateway.



4.2 Preparations for Login

Modify the IP address of the PC to make it at the same network segment with the DAG1000-4S device, since the default IP address of the gateway is 192.168.100.1.

Take Windows 11 as an example, the IP address of PC is changed into 192.168.100.3:



Check the connectivity between the PC and the gateway. Click **Start -> Run** of PC and enter cmd to execute 'ping 192.168.100.1' to check whether the IP address of the DAG1000-4S gateway runs normally.

4.3 Log in Web Interface

Open a web browser and enter the IP address of the LAN port of the gateway (the default IP of LAN port is 192.168.100.1, while that of WAN port is obtained via DHCP by default). Then the login GUI will be displayed.

It is advised to modify the username and password for security consideration.

Web Management System

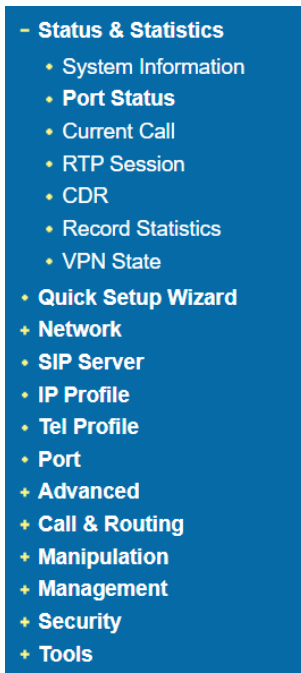
Enter default username and password: admin/admin@123#, then click "**Login**" to enter into the Web interface.



4.4 Navigation Tree

The web management system of the DAG1000-4S VoIP gateway consists of the navigation tree and detailed configuration interfaces.

Choose a node of the navigation tree to enter into a detailed configuration interface.



4.5 State and Statistics

4.5.1 System Information

On the System Information interface, you can view the information of device ID, MAC address, network mode, IP addresses, version information, sever register status and so on.

System Information

Device ID	0123-4567-89ab-cdef		
MAC Address	F8-A0-78-66-78-33		
Network Mode	Bridge		
IP Address	172.27.11.95	255.255.0.0	Static
	172.27.1.1		
DNS Server	114.114.114.114	4.4.4.4	
Cloud Register Status	Not Registered		
NMS Register Status	Not Registered		
System Uptime	14 h: 21 m: 37 s		
System Time	2025-9-11 23:21:27		
Traffic Statistics	Received 27328791 bytes	Sent 5624229 bytes	
Usage of Flash	93 %(7421952 / 7929856) bytes		
Usage of Backup Flash	37 %(5476352 / 14680064) bytes		
Usage of RAM in Linux	40 %(24424448 / 60112896) bytes		
Usage of RAM in AOS	77 %(13041664 / 16769024) bytes		
Current Software Version	DAG1000-4S 2.83.13.05 -DEBUG PCB 48 LOGIC 0 BIOS 1, 2025-09-11 19:46:48		
Backup Software Version	DAG1000-4S 2.83.13.05 -DEBUG PCB 48 LOGIC 0 BIOS 1, 2025-09-11 14:35:50		
DSP Version	ARM_32_13 Jan 13 2022 17:39:22		
U-BOOT Version	23		
Kernel Version	27		
Root FS Version	23		
FS Version	22		
Hint Language	Chinese		

Figure 4.5- 1 System Information

Explanation of items on System Information interface

Device ID	A unique ID of each device. This ID is used for warranty and cloud server authentication.
MAC address	Hardware address of the WAN port
Network Mode	Network modes include bridge and router. Under the Bridge mode , the network port will work as a small LAN switch. Under the Router Mode , NAT feature will be enabled under this mode.

IP Address	The IP address of the WAN port of the gateway is shown. DHCP: Obtain IP address automatically. DAG1000-4S is regarded as a DHCP client, which sends a broadcast request and looks for a DHCP server from the LAN to answer. Then the first discovered DHCP server automatically assigns an IP address to the DAG1000-4S from a defined range of numbers. Static IP Address: Static IP address is a semi-permanent IP address and remains associated with a single computer over an extended period of time. This differs from a dynamic IP address, which is assigned <i>ad hoc</i> at the start of each session, normally changing from one session to the next. If you choose static IP address, you need to fill in the following information: • IP Address: the IP address of the WAN port of the DAG1000-4S; • Subnet Mask: the netmask of the router connected the DAG1000-4S; • Default Gateway: the IP address of the router connected the DAG1000-4S; PPPoE: PPPoE is an acronym for point-to-point protocol over Ethernet, which relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. PPPOE IP address refers to IP address assigned through the PPPoE mode. If you choose PPPoE, you need to fill in to fill in the following information: • Username: the account name of PPPoE • Password: the password of PPPoE • Server Name: the name of the server where PPPoE is placed
DNS Server	IP address of DNS server and default gateway information is displayed.
Cloud Register Status	Whether the DAG1000-4S gateway is registered to cloud or not.

NMS Register Status	Whether the DAG1000-4S gateway is registered to NMS or not.
System Uptime	The running time of the DAG1000-4S since it is powered on.
System Time	System time can be synchronized with an NTP server according to the time zone or directly with the local browser time.
Traffic Statistics	Total bytes of message received and sent by network port.
Usage of Flash	Detailed usage of Flash memory
Usage of Backup Flash	Detailed usage of Backup Flash memory
Usage of RAM in Linux	Detailed RAM usage of Linux core
Usage of RAM in AOS	Detailed RAM usage of AOS
Current Software Version	The software version that runs on the gateway. Model name, version number and the software development date are displayed.
Backup Software Version	Backup software is for the purpose of backup. When the current software fails, the backup software version will work.
DSP Version	DSP version
U-boot Version	U-boot version
Kennel version	Linux Kennel version
Root FS Version	Root file system version
FS Version	File system version
Hint Language	The current language of the DAG1000-4S gateway

4.5.2 Port Status

On the **Status & Statistics -> Port Status** page, users can view the registration status of each port and port group, as well as the port call status, voltage, current, and other related information.

User status:

- ✧ Registered: the port is registered to SIP server successfully;
- ✧ Unregistered: the port fails to be registered to SIP server.

Port								
Port No.	Type	SIP User ID	User Status	Port Status	Voltage	Current	Call Status	Operate
1	FXS	---	---	OnHook	47V	0mA	Idle	---
2	FXS	---	---	OnHook	47V	0mA	Idle	---
3	FXS	1058190002	Not Registered	OnHook	47V	0mA	Idle	---
4	FXS	---	---	OnHook	47V	0mA	Idle	---

Port Group			
Group	Port	SIP User ID	User Status
7 <123>	0,1,...	1058190001...	Not Registered

Figure 4.5- 2 Port and Port Group Status

4.5.3 Current Call

Current Call					
Port	Type	Source	Destination	Connected Time	Duration(s)
---	---	---	---	---	---

Refresh

Figure 4.5- 3 Current Call Information

The interface above displays real-time connection information for the current call.

4.5.4 RTP Session

RTP Session													
Port	Source	Destination	Payload Type	Packet Period	Local Port	Peer IP	Peer Port	Sent Packets	Recv Packets	Lost Packets Rate(%)	Jitter	Duration(s)	
---	---	---	---	---	---	---	---	---	---	---	---	---	---

Refresh

Figure 4.5- 4 RTP Session

The above interface shows real-time RTP session information, including: port, source, destination, payload type, packet period, local port, peer IP, peer port, sent packets, receive packets, lost packets, jitter and duration.

4.5.5 CDR

CDR (Call Detail Record): is a data record produced by a telephone exchange or a communication device, which contains the details of a telephone call that passes through the device.

CDR

Enable CDR

☐ No
 ☒ Yes

save

Start Date

202

6

2

End Date

202

6

24

Port

All

Call State

All

Source

Destination

CDR Oper

Export

filter

Clear

Enable Advanced Option

☒ No
 ☐ Yes

Total : 0 Entry - 50 Entry/Page - 1/1

Page 1

Port	Start Time	Answer Time	Direction	Source	Destination	PeerIP	Codec	Reason	Duration (s)
------	------------	-------------	-----------	--------	-------------	--------	-------	--------	--------------

Figure 4.5- 5 CDR

On the **Status & Statistic -> CDR** interface, details of all calls through the ports of the DAG1000-4S are displayed. The CDR function can be enabled on this interface.

4.5.6 Record Statistics

On the **Status & Statistic -> Record Statistics** page, record statistics including server status, count of current records, count of no response, count of server return errors, count of record starts, count of record startAck, count of record stops and count of stopAck are displayed.

Record Statistics							
Server Stat	Current Records	No Responses	Server Return Error	Start	StartAck	Stop	StopAck
Not Config	0	0	0	0	0	0	0

No Response Statistics	
Link Dect NoRsp Cnt	0
Start Time Out Cnt	0
Rel Call Before StartAck	0
Stop Time Out Cnt	0

Refresh

Reset

Figure 4.5- 6 Record Statistics

4.5.7 VPN State

On the **Status & Statistic -> VPN State** page, we can view the status of the VPN connection. VPN state information including: Protocol, state (VPN availability), IP Address of the gateway which assigned by VPN server, Gateway, Server Address for VPN server, RX / TX Bytes, Connection Status and Login Time.

VPN State							
Protocol	State	IP Address	Gateway	Server Address	RX / TX Bytes	Connection Status	Login Time
udp	disable	--	--	--	0/0	offline	0.0.0 0:0:0

Figure 4.5- 7 VPN State

4.6 Quick Setup Wizard

Quick setup wizard guides user to configure the device step by step. User only needs to configure network, SIP server and SIP port in the Quick Setup Wizard interface. Basically, after these three steps, user is able to make voice call via the DAG1000-4S device.

4.7 Network Configuration

4.7.1 Local Network

The DAG1000-4S gateway has two kinds of network mode: route and bridge. When the gateway works under the route mode, it will work as a small router and NAT function is enabled. Under this situation, WAN port is normally connected to router/switch or ADSL MODEM, while LAN port is connected local computer or other network device (such as Ethernet switches, Hubs etc.).

When the gateway works under the bridge mode, WAN port and LAN port are the same. The gateway serves as a two-port Ethernet switch. Under this network mode, user only needs to configure the IP address of WAN port and DNS.

DHCP:

Obtain IP address automatically.

Static IP Address:

Static IP address is a permanent IP address which is assigned by Internet Service Provider (ISP) and remains associated with a single computer over an extended period of time. This differs from a dynamic IP address, which is assigned ad hoc at the start of each session, normally changing from one session to the next.

PPPoE:

PPPoE is an acronym for point-to-point protocol over Ethernet, which relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections. PPPOE IP address refers to IP address assigned through the PPPoE mode.

If you choose PPPoE, you need to fill in the account, password and service name, which are provided by telecom operator.

Local Network

IP Protocol

IPv4

Network Mode

☒ Router
☐ Bridge

WAN Port

☐ Obtain an IP address automatically
☒ Use the following IP address

IP Address

172.27.180.181

Subnet Mask

255.255.0.0

Default Gateway

172.27.1.1

☐ PPPoE

Account

Password

Service Name

WAN MTU

1500

LAN Port

IP Address

192.168.100.1

Subnet Mask

255.255.255.0

LAN MTU

1500

DNS Server

☐ Obtain DNS server address automatically
☒ Use the following DNS server address

Primary DNS Server

114.114.114.114

Secondary DNS Server

4.4.4.4

Note:The device must restart to take effect.

Figure 4.7- 1 Route Mode

25

User Manual

Shenzhen Dinstar Co.,Ltd.

 www.dinstar.com

Local Network

IP Protocol

IPv4

Network Mode

☐ Router
☒ Bridge

Network Configuration

☐ Obtain an IP address automatically
☒ Use the following IP address

IP Address

172.27.11.95

Subnet Mask

255.255.0.0

Default Gateway

172.27.1.1

☐ PPPoE

Account

Password

Service Name

WAN MTU

1500

Manage Address

IP Address

Subnet Mask

DNS Server

☐ Obtain DNS server address automatically
☒ Use the following DNS server address

Primary DNS Server

8.8.8.8

Secondary DNS Server

4.4.4.4

Figure 4.7- 2 Bridge Mode

Note:

- If DHCP is selected to obtain IP address, please ensure DHCP server in the network works normally.
- When the gateway works under the route mode, the IP address of LAN port and that of WAN port cannot be at the same network segment, otherwise the gateway can't work normally.
- When the gateway works under the route mode, log in the gateway's web configuration interface via the LAN port.
- After the configurations are finished, please restart the gateway for the configurations to take effect.

4.7.2 VLAN (Virtual Local Area Network)

In order to control the impacts brought by broadcast storms, user can divide VLANs into three groups, namely VLAN1, VLAN2 and VLAN3. There are kinds of VLAN, including data VLAN, voice VLAN and management VLAN. Different kind of VLAN has different messages.

► 802.1Q (VLAN ID)

The IEEE 802.1Q standard defines the architecture for Virtual Bridged LANs, the services provided in Virtual Bridged LANs and the protocols and algorithms involved in the provision of those services.

No Quality of Service mechanisms are defined in this standard, but an important requirement for providing QoS is included in this standard, e.g. the ability to regenerate user priority of received frames using priority information contained in the frame and the User Priority Regeneration Table for the reception Port.

► 802.1P (Priority)

IEEE 802.1P standard, describes important methods for providing QoS at MAC level. IEEE 802.1p is in fact quite good. Lower priority level packets are not sent, if there are packets in queued in higher level queues. IEEE 802.1p describes no admission control protocols. It would be possible to give Network Control priority to all packets and the network would be easily congested.

VLAN

VLAN NO.

0

☐ Data
 ☒ Voice
 ☒ Mngt

VLAN ID(1 - 4095)

Priority(0 - 7)

Network Configuration

☒ Obtain an IP address automatically
 ☐ Use the following IP address

IP Address

Subnet Mask

Default Gateway

DNS Server

☒ Obtain DNS server address automatically
 ☐ Use the following DNS server address

Primary DNS Server

Secondary DNS Server

MTU

1400

Figure 4.7- 3 VLAN parameter configuration

Explanation of the parameters in VLAN interface:

Data/Voice/Management	If the checkboxes on the right of data, voice and management of VLAN1 are selected, it means data messages, voice messages and management messages are subject to the network setting, 802.1Q VLAN1 ID and 802.1P Priority of VLAN1.
VLAN ID (0-4095)	Set an ID to identify a VLAN based on 802.1Q protocol.
Priority (0-7)	Set the priority of a VLAN based on 802.1P protocol.
Network Configuration/DNS Server	Set a DHCP IP address or static IP address for a VLAN, and set the IP address of the DNS server used by the VLAN.

Note:

User needs to restart the gateway for the configurations to take effect.

4.7.3 DHCP Option

When the DAG1000-4S device works as a DHCP client and applies for an IP address, DHCP server will return packets which include an IP address as well as configuration information of enabled option fields.

The following is the meaning of the option fields involved in DAG1000-4S (that means the following option fields are enabled, DHCP server will return information of corresponding option fields:

- Option 15: to set a DNS suffix;
- Option 42: to specify NTP server;
- Option 60: to define VCI (vendor class identifier) of DAG1000-4S on the DHCP server;
- Option 66: to specify TFTP server which will assign software version to DAG1000-4S;
- Option 120: to fetch SIP server address;
- Option 121: to obtain classless static route. DAG1000-4S will add these static routes to the static route table after it fetches them from DHCP server.

DHCP Option

Option 15 (Domain Name)	
Option 42 (NTP Servers)	☐ Enable
Option 60 (Class Identifier)	
Option 66 (TFTP Server)	☐ Enable
Option 120 (SIP Server)	☐ Enable
Option 121 (Classless Static Route)	☐ Enable

Save

Figure 4.7- 4 DHCP Option Configuration

4.7.4 QoS

The DAG1000-4S device can label QoS priority on the IP messages it sends out, so as to resolve network delay or network congestion. Meanwhile, the device can give different QoS tags for management-related packets of Web/Telnet, voice packets and signal packets.

Qos

DSCP code point is used for diffserv setting. It utilizes the first 6 bits of IP ToS. The default values are EF(184), AF1(1),AF2(2), AF3(3), AF4(4), BE(0). You can use different DSCPs for voice or data based on the network provider.

Set DSCP Code/IP ToS

☒ Enable

Manage(WEB/Telnet):

0

Voice Packet:

0

Signal Packet:

0

Figure 4.7- 5 QoS Configuration

4.7.5 DHCP Server (Route Mode)

When the gateway works under the route mode, it works as a small router and user can its DHCP service so that the DAG1000-4S serves as a DHCP server in the network.

- “Start address” and “end address” of the address pool determine the range of IP addresses which are automatically assigned to other devices.
- “IP Expire Time” means the service time of an assigned IP address. When the service time expires, the IP address will no longer be by the network equipment.
- The subnet mask, gateway, DNS and other information will be transferred to the network equipment through the DHCP protocol.

DHCP Server

DHCP Server

☒ Enable

IP Pool Starting Address

192.168.100.100

IP Pool Ending Address

192.168.100.199

IP Expire Time

72

h

Subnet Mask (Optional)

255.255.255.0

Default Gateway (Optional)

192.168.100.1

Primary DNS Server (Optional)

192.168.100.1

Secondary DNS Server (Optional)

Figure 4.7- 6 DHCP Server

Note:

When configuring the start IP address, end IP address, subnet mask and gateway IP address, please set them at the same network segment with the IP address of LAN port. Otherwise, other devices under the network will not work normally after they get the IP address assigned by the DHCP server. After the configurations are finished, please restart the DAG1000-4S for the configurations to take effect.

4.7.6 DMZ Host (Route Mode)

If the DMZ service is enabled, the devices in the wide-area network are allowed to have direct access to the devices in the DMZ (demilitarized zone). In this way, devices in the wide-area network can visit the devices which are in the local area network and meanwhile the devices in the local area network are protected.

DMZ Host

DMZ Host IP Address

☐ Enable

Note:The IP address needs to be in the same subnet with LAN port.

Save

Figure 4.7- 7 DMZ Host

Note:

After the configurations are finished, please restart the DAG1000-4S for the configurations to take effect.

4.7.7 Forward Rule (Route Mode)

Sometimes, a device under the LAN network needs to provide a port for communication with the WAN network (such as providing the port 21 for FTP service). In those cases, user can configure forwarding rules for that network device.

Forward Rule				
ID	Server Port	IP Address	Protocol	Enable
1			TCP v	☐
2			TCP v	☐
3			TCP v	☐
4			TCP v	☐
5			TCP v	☐
6			TCP v	☐
7			TCP v	☐
8			TCP v	☐

Note:1.'IP Address' needs to be in the same subnet with LAN port.
2.'Server Port' range: 0 - 65535, The services port(like telnet,web,sip,rtp,provision and so on) can not be configured.

Figure 4.7- 8 Forward Rule

Service port is the port that provides service for the WAN network, while IP address is the IP address of the network device under the LAN network. The protocol is TCP or UDP.

The different between forwarding rule and DMZ host is that DMZ Host offers all ports (0-1024) and protocols for outside telecommunication while forwarding rule only offers a single or several ports and protocols of TCP or UDP.

Note:

When both DMZ Host and forwarding rule are configured, the configuration of forwarding rule is prior to that of DMZ Host.

4.7.8 Static Route (Route Mode)

Static route determines the routing rule during the handling of messages by the gateway. Most of time, user does not need to configure static route. Only when there are multiple network segments in the LAN network and these segments need to complete some specific applications, static route needs to be configured.

ID	Dest. IP Address	Subnet Mask	Nexthop	Enable
1				☐
2				☐
3				☐
4				☐
5				☐
6				☐
7				☐
8				☐

Figure 4.7- 9 Static Route

4.7.9 Firewall-Forward Rule (Route Mode)

The firewall filters information sent from MAC addresses and domain names, and via routing mode to filter source and destination IP addresses within a specified IP range.

Firewall-Forward Rule							
IP Filter							☒ Enable
ID	Source IP	Source Port	Destination IP	Destination Port	Protocol	Status	
---	---	---	---	---	---	---	
Add Mod Del							
MAC Filter							☒ Enable
ID	MAC	Describe	Status				
---	---	---	---				
Add Mod Del							
Domain Filter							☒ Enable
ID	Domain	Status					
---	---	---					
Add Mod Del							
Save							

Figure 4.7- 10 Firewall-Forward Rule

4.7.10 ARP

ARP is address resolution protocol. ARP helps user get the MAC address of a device through its IP address. Under TCP/IP network environment, each host is assigned with a 32-bit IP address, but MAC address needs to be known for message transmission in the physical network. ARP is a tool that converts IP address into MAC address.

ARP	
Type	☒ Static ☐ Dynamic
IP Address	MAC Address
---	---
Total: 0 entry ▼	

Figure 4.7- 11 ARP Parameters

4.7.11 VPN

OpenVPN is an open-source virtual private network (VPN) protocol widely used to establish secure point-to-point or remote access connections. This VPN feature allows users to create a secure remote network connection by configuring the protocol, server address, authentication information, and uploading certificates. It can encrypt data transmission, protect user privacy and network security, and ensure authentication and access control.

VPN	
Mode	File Import Mode(.ovpn) ▼
State	Disable ▼
Ignore Route Configuration issued by the server	☒ Enable
Authentication Username	
Authentication Password	
Certificate	Choose File No file chosen

Figure 4.7- 12 VPN-File Import Mode

VPN

Mode

Advanced Mode

State

Disable

Ignore Route Configuration issued by the server

☒ Enable

Protocol

udp

Device

tun

Authentication Username

Authentication Password

Remote Server Address

Remote Server port

0

Secondary Server Address

Secondary Server port

0

Root Certificate

Choose File

No file chosen

Client Certificate

Choose File

No file chosen

Client Key

Choose File

No file chosen

Note: The device must restart to take effect.

Figure 4.7- 13 VPN-Advanced Mode

Explanation for VPN parameters:

Mode	File import (.ovpn) or Advanced
State	Disable or Enable VPN
Ignore Route Configuration issued by the server	Choose whether to ignore the default route pushed by the server. If enabled, the server's default route will be ignored
Accept Push Route	Choose whether to accept routes pushed by the server. When enabled, the device can access routes the server pushes
Protocol	Select UDP or TCP; this must match the VPN server's protocol
Device	Choose tun (routing) or tap (bridging); must match VPN server setting
Authentication Username	Username for authentication. Usually the certificate may include this so it can be left blank
Authentication Password	Password for authentication. Usually the certificate may include this so it can be left blank
Remote Server Address	OpenVPN server address (hostname or IP)
Remote Server port	OpenVPN server port

Secondary Server Address	Backup OpenVPN server address (secondary/alternative server)
Secondary Server port	Backup OpenVPN server port
Root Certificate	Root CA certificate; same root certificate used on the server side. The root certificate for users under the same server is identical
Client Certificate	each user normally has a distinct client certificate

4.8 SIP Server

Introduction of SIP Server:

- 1) SIP server is the main component of VoIP network and is responsible for establishing all the SIP calls. SIP server is also called SIP proxy server or register server. Both IPPBX and softswitch can act as the role of SIP server.
- 2) Usually, SIP server does not participate in media processing. Under SIP network, media always use end-to-end negotiating. Simple SIP server is only responsible for the establishment, maintenance and cleaning of sessions, while relatively-complex SIP server (SIP PBX) not only provides basic calling and conversational support, but also offers rich services such as Presence, Find-me and Music On Hold.
- 3) SIP server based on Linux platform, such as: OpenSER、sipXecx、VoS、Mera etc.
- 4) SIP server based on windows platform, such as: mini SipServer, Brekeke, VoIPswitch, etc.
- 5) Carrier-grade soft switch platform, such as Cisco, Huawei, ZTE etc.

SIP Server

IP Protocol for SIP Stack

IPv4

SIP Server

SIP Server

172.27.123.124

SIP Server Port (Default: 5060)

5064

Registration Expires (Default: 300)

300

s

Heartbeat

☐ Enable

Primary Outbound Proxy

Primary Outbound Proxy Address

Primary Outbound Proxy Port

5060

Secondary Outbound Proxy

Secondary Outbound Proxy Address

Secondary Outbound Proxy Port

5060

Registration

Re-registration Percent(Expires)(0: means random, range: 25%-75%)

0

Retry Interval when Registration failed

30

s

Registration Limit (counts/time, time: 0 means unlimited)

1 / 0

s

Send SIP Unregistration Request when the Device Restart

☐ Enable

MOH

MOH Dial Number

☐ Enable

~~mh~u

SIP Transport Type

UDP

Local SIP Port

Use Random Port

☐ Enable

SIP UDP/TCP Local Port

5060

SIP Protocol Stack Startup Protection

Reboot After Stack Consecutive Startup Failures(0: means no reboot)

0

Times

Figure 4.8- 1 Configuration Interface for SIP Server

Explanation for SIP parameters:

IP Protocol for SIP Stack	Choose SIP protocol stack, support IPv4 and IPv6, please choose the corresponding protocol according to the actual connected server
SIP Server	The IP address or domain name of the SIP server. They are provided by VoIP service provider.
SIP Server port	The Service port of the SIP server. It is 5060 by default.

Registration Expires	It is used to avoid excessively frequent registrations. When the time that is set expires, terminals will send register request to the SIP server. The time is 1800s by default.
Heartbeat	Heartbeat is used to check the connection between terminal and SIP server.
Primary Outbound Proxy Address	The IP address or domain name of primary outbound proxy server, which is provided by service provider.
Primary Outbound Proxy Port	The service port of the primary outbound proxy server. Default outbound proxy port is 5060.
Secondary Outbound Proxy Address	The IP address or domain name of secondary outbound proxy server, which is provided by service provider.
Secondary Outbound Proxy Port	The service port of the secondary outbound proxy server. Default outbound proxy port is 5060.
Re-registration Percent (Expires)	After a specified interval (registration expires * re-registration percent), the terminal resends the registration request to the server (default 0 means random).
Retry Interval when Registration failed	The retry interval time after a registration fails. Default: 30s
Registration Limit	The maximum number of registrations in a second. 0 means no limitation for registrations.
Send SIP Unregistration Request when the Device Restart	All SIP accounts are logged out and then re-registered after the device is rebooted
MOH	The MOH (Music on Hold) feature provides music play to callers when their call is placed on hold. When enabled, users can configure the number to call on hold.
MOH Dial Number	Initiating a call to a set number after the call is placed on hold
SIP Transport Type	The way of SIP-based transmission. It can be UDP, TCP and Auto. Default: UDP.
Use Random Port	The SIP port for providing services for terminal is chosen by random.
SIP UDP/TCP Local Port	The UDP/TCP port of DAG1000-4S device for using SIP services. Default SIP UDP/TCP local is 5060.
SIP TLS Local Port	The TLS port of DAG1000-4S device for using SIP services. Default SIP TLS local port is 5061.
Reboot After Stack Consecutive Startup Failures	If the stack fails to start consecutively due to specific reasons and the failure count reaches the configured threshold, restart the device.

4.9 IP Profile

The device supports simultaneous registration to multiple SIP servers and making calls. Different ports can be configured with different SIP server addresses and use different voice codecs as needed. IP profiles are used to create SIP server addresses, proxy servers, dialing rules, service parameters, dialing parameters, voice codec and other parameter configuration for ports. When configuring the port, you can save the IP profile index and use it. For index configuration, refer to the "Port " page.

When the device is only registered to one SIP server, the IP profile does not need to be configured, and the default IP profile can be used. When the device needs to register to multiple SIP servers, click the "Add" button to create a new IP profile, as shown in the figure below:

IP Profile												
☐	Index	Description	SIP Server	SIP Server Port	Registration Expires	Heartbeat	Primary Outbound Proxy Address	Primary Outbound Proxy Port	Secondary Outbound Proxy Address	Secondary Outbound Proxy Port	DTMF Method	Preferred Vocoder
☐	0	default	172.27.123.124	5064	300	Disable	---	5060	---	5060	RFC2833	G.711U

Add

Modify

Delete

IP Profile - Add

Index	1
Description	
SIP Server	
SIP Server Address	
SIP Server Port (Default: 5060)	5060
Registration Expires (Default: 300)	300 s
Heartbeat	☐ Enable
Primary Outbound Proxy	
Primary Outbound Proxy Address	
Primary Outbound Proxy Port	5060
Secondary Outbound Proxy	
Secondary Outbound Proxy Address	
Secondary Outbound Proxy Address	
MOH	☐ Enable
MOH Dial Number	~~mh~u
Digit Map	
Match Failed(When the registration is successful)	Send to the server
Digit Map	
<pre>[*#]T [*#][*#] *x.T **x.# [*#]xx# *#xx# [*#][0-9*#]x[0-9*].x# x.# x.T</pre>	

Service Parameter

SUBSCRIBE for MWI(Message Waiting Indicator) ☐ Enable
MWI Subscription Expires(Default: 3600) s
Voicemail User ID

Echo Cancel Tail ms

SIP Compatibility

PRACK(RFC3262) ☐ Enable
PRACK Only for 18x with SDP ☐ Enable
Early Media ☒ Enable
Early Answer ☐ Enable

DTMF Parameter

DTMF Method
RFC2833 Payload Type Preferred(Incoming Call)
RFC2833 Payload Type
DTMF Gain
RTP Event of Flash

Send Flash Event ☐ Enable
Send DTMF Tone to Analog When Call in Active ☒ Enable

Codec Parameter

Codecs Preferred

	Coder Name	Payload Type	Packetization Time(ms)	Rate(kbps)	Silence Suppression
1	G.711U	0	20	64	Disable
2	G.711A	8	20	64	Disable
3	G.729	18	20	8	Disable
4	G.723	4	30	63	Disable
5					

Encryption Configuration

SIP Encrypt
RTP Encrypt
Encrypt Mode

Figure 4.9- 1 IP Profile Configuration

4.10 Tel Profile

The device supports setting different values for the line parameters to each port. Different ports can be configured with different gains and fax parameters as needed. Tel profile is used to create a configuration group of line parameters, service parameters, and fax parameters for the port. During port configuration, you can save the Tel profile index and use it. For index configuration, refer to the "Port " page.

Under normal circumstances, the Tel profile does not need to be configured, and the default Tel strategy can be used.

When you need to set different line parameters, business modes, or fax modes for different ports, you can add Tel profile through the "Add" button. As shown below:

Tel Profile											
Index	Description	Work Mode	Voice Output Mod	Config Mode(Gain)	Tx Gain(IP->PSTN)	Rx Gain(PSTN->IP)	Fax Mode	ECM	Rate	Tone Detection by	Switch into Fax Mode When Detected CNG or CED
☐ 0	default...	Voice and Fax	Telephone	Basic	+4dB	0dB	Adaptive	Disable	14400bps	Local	Disable

Tel Profile - Add

Index

1

Description

Line Parameter

Work Mode

Voice and Fax

Voice Output Mod

☒ Telephone
 ☐ Headset

Config Mode(Gain)

☒ Basic
 ☐ Advanced

Tx Gain(IP->PSTN)

+4dB

Rx Gain(PSTN->IP)

0dB

Send CID before Ringing

☐ Enable

Delay of Sending CID after Ringing

500

ms

Service Parameter

Visual MWI Type

NEON

NEON Voltage(75-100V)

90

FAX Parameter

Fax Mode

Adaptive

Include "a=X-fax" Attribute

☐ Enable

Include "a=fax" Attribute

☐ Enable

Include "a=X-modem" Attribute

☐ Enable

Include "a=modem" Attribute

☐ Enable

Include "vbd" Parameter

☒ Enable

Include "silenceSupp" Parameter

☒ Enable

ECM

☐ Enable

Rate

14400 bps

Transport

udptl

Tone Detection by

Local

Switch into Fax Mode When Detected CNG or CED

☐

FXS Param

Long Line Support

☐ Enable

Figure 4.10- 1 Tel Profile Configuration

4.11 Port

A unique SIP account used for registration can be configured for each FXS port of DAG1000-4S device. Parameters of the SIP account include port number, whether to register, display name, SIP user ID, Authenticate ID, Authenticate password, off-hook auto-dial number, caller ID and so on.

Port Add

Port

1

Disable Port

☐

Registration

☒ Enable

IP Profile

0 <default>

Tel Profile

0 <default>

Display Name

SIP User ID

Authenticate ID

Authenticate Password

Offhook Auto-Dial

Auto-Dial Delay Time

s

DND(Do Not Disturb)

☐ Enable

Caller-ID

☒ Enable

Number for CFU(Call Forwarding Unconditional)

Number for CFB(Call Forwarding Busy)

Number for CFNRy(Call Forwarding No Reply)

Call Waiting

☐ Enable

Play Call Waiting Tone

☐ Enable

Call Waiting Send CID

☐ Enable

Figure 4.11- 1 Port Configuration Interface

Explanation for port parameters:

Port	Port number
Disable port	Whether to disable port temporally
Registration	Whether to enable registration for the port

IP Profile	IP profile (need to be created in advance, refer to 4.9 IP profile configuration)
Tel Profile	Tel Profile (need to be created in advance, refer to 4.10 IP policy configuration)
Display Name	Description of SIP account. It is used to identify the SIP account.
SIP User ID	User ID of the SIP account, which is provided by VoIP service provider (ITSP) for registration. Usually it is in the form of digits similar to phone number or an actual phone number.
Authenticate ID	SIP service subscriber's authenticate ID used for authentication. It can be identical to or different from SIP User ID.
Authenticate password	SIP password which registers to soft switch/SIP server
Offhook Auto-dial	An extension or phone number is pre-assigned here so that the number is automatically dialed as soon as user picks up the phone
Auto-dial Delay Time	How long the auto-dial number is prolonged. If it is set as 3s, the auto-dial number is dialed after 3 seconds pass.
DND (Do Not Disturb)	The phone won't receive any calls in case it enabled
Caller ID	Enable or disable caller ID for corresponding port. If it is disabled, the caller ID for the calls through the port won't be displayed.
Number for CFU	Call forward unconditional. All incoming calls will be forwarded to pre-assigned number automatically
Number for CFB	Call forward on busy. If the line is busy, the call will be forwarded to pre-assigned number automatically
Number for CFNRy	Call forward no reply. If the call is not answered, the call will be forwarded to pre-assigned number automatically
Call Waiting	If call waiting is enabled, a special tone is sent if another caller tries to reach you
Play Call Waiting Tone	If call waiting tone is enabled, caller will hear special tone.
Call Waiting Send CID	When enabled, caller ID is displayed during call waiting

4.12 Advanced

4.12.1 Line Parameter

On the **Advanced ->Line Parameter** page, you can configure line parameters which include for call progress tone, auto gain control, fax parameters and so on.

Line Parameter

Call Progress Tone

UK

Ring Back Tone

400,180,450,180,400,200,400,2000

Busy Tone

400,180,400,630,375,375,0,0

Dial Tone

350,180,440,180,0,0,0,0

Call Waiting Tone

Call Waiting Tone Duration

800

ms

Call Waiting Tone Gap

2000

ms

Call Waiting Tone Repeat Count

5

Auto Gain Control

IP->PSTN

☐ Enable

PSTN->IP

☐ Enable

DSP Jitter Buffer(Recv) Config Mode

Adapter

Buffer Size

20

ms

Line Parameter

Work Mode

Voice and Fax

Voice Output Mod

☒ Telephone
 ☐ Headset

Config Mode(Gain)

☒ Basic
 ☐ Advanced

Tx Gain(IP->PSTN)

+4dB

Rx Gain(PSTN->IP)

0dB

FAX Parameter

Fax Mode

Adaptive

Include "a=X-fax" Attribute

☐ Enable

Include "a=fax" Attribute

☐ Enable

Include "a=X-modem" Attribute

☐ Enable

Include "a=modem" Attribute

☐ Enable

Include "vbd" Parameter

☒ Enable

Include "silenceSupp" Parameter

☒ Enable

ECM

☐ Enable

Rate

14400 bps

Transport

udptl

Tone Detection by

Local

Switch into Fax Mode When Detected CNG or CED

☐

Figure 4.12- 1 Line Parameter Configuration

Explanation for FXS parameters:

Call Process Tone	The signal tone standard after a phone is picked up. Choose national standards from the drop-down box. Default value is UK.
Call Waiting Tone	Set the duration, interval and number of repetitions for the

	call waiting tone
Auto Gain Control	Whether to enable automatic gain control
DSP Jitter Buffer (Recv) Config Mode	It supports two modes, static and adapter
Work Mode	To set the FXS ports work in both Voice and Fax mode. There are several configure options: • Voice and FAX: to be able to make call and use FAX service • Voice Only: allows to make call only, Fax doesn't work if you connect a fax machine • Fax Only: allows to make Fax call only. • POS only: allows to connect POS terminal only
Voice Output Mod	It supports two voice output modes: telephone and headset
Config Mode (Gain)	TX Gain (PSTN -> IP): adjust gain value from analog phone RX Gain (IP -> PSTN): adjust gain value to analog phone
FAX Parameter	The DAG1000-4S device supports the three fax modes: T.38 (IP-based), T.30 (Pass-Through) and Adaptive Fax Mode (automatically match with the peer fax mode).
Fax Mode	There are three fax modes: T.38, T.30(Pass-through), and Adaptive.
Include "a=X-fax" Attribute	If this parameter is enabled, "a=X-fax" attribute will be carried in SDP
Include "a=fax" Attribute	If this parameter is enabled, "a=fax" attribute will be carried in SDP
Include "a=X-modem" Attribute	If this parameter is enabled, "a=X-modem" attribute will be carried in SDP
Include "a=modem" Attribute	If this parameter is enabled, "a=modem" attribute will be carried in SDP
ECM	Whether to enable 'Error Correction Mode' (ECM) .
Rate	The rate of sending or receiving fax, default value is 14400bps.
Transport	The transport protocol used for fax control: udptl, tcp, rtp
Tone Detection by	Fax sound is detected by caller, callee or automatically.
Switch into Fax Mode When Detect CNG or CED	If this parameter is enabled, the system will switch into fax

	mode when CNG or CED is detected.
--	-----------------------------------

4.12.2 FXS Parameters

FXS parameters include: timeout Call Progress Tone, Timeout for Dialing, Send Polarity Reversal etc.

FXS Parameter	
Send Polarity Reversal	☐ Enable
Detect Hook Flash	☒ Enable
Min Time	100 ms
Max Time	400 ms
Ringing Tone	0,0,0,0,0
CID Type	FSK
Modulation Type	BFSK Bel202
Message Type	MDMF
Message Format	Display Name and CID
Send CID before Ringing	☐ Enable
Delay of Sending CID after Ringing	500 ms
Caller Number Preferred when FXS Call Out	Adaptive
CFNRy Timeout	33 s
SLIC Setting	600 Ohm
REN	4
Current Threshold(Off-Hook -> On-Hook)	10 mA
Current Threshold(On-Hook -> Off-Hook)	12 mA
Port Current Protection Threshold(0: means disable)	0 mA
Current of Off-Hook(Non-long Line)	20mA
Long Line Support	☐ Enable

Figure 4.12- 2 Configuration Interface for FXS Parameters

Explanation for FXS parameters:

Send Polarity Reversal	If polarity reversal is enabled, call tolls will be calculated based on the changes in voltage. If polarity reverse is disabled, you need to set the time for offhook detection and call tolls will be calculated starting from the set time.
Detect Hook flash	If 'Detect Hook Flash' is enabled, you need to set a minimum time and a maximum time. If a phone's hook flash is pressed for a time period greater than the set minimum time but less than the maximum time, the action is considered as a 'hook flash' operation. If a phone's hook flash is pressed for more the set maximum time, the action is considered as 'hang up the phone'.
Ringing Tone	Set ringing tone for gateway
CID Type	There are two CID types, namely DTMF and FSK.

Modulation Type	There are two modulation types, namely BFSK Bel202 and CCITT V.23
Message Type	There are two call display types including SDMF and MDMF
Message Format	The call display format in analog phone. It can be "Display Name and CID", "CID only", or "Display Name only"; default value is "Display Name and CID"
Send CID before Ringing	If this parameter is enabled, the gateway send Caller ID to phone before ringing, otherwise the caller ID will be displayed after ringing.
Delay of sending CID after Ringing	The time how long the caller ID will be delayed when the caller ID is set to be displayed after ringing. Default value is 500ms.
Caller Number Preferred when FXS Call Out	Users can configure the primary caller number that will be called out to the target number in priority. Users can select Adaptive, Port Account or Port Group Account
CFNRy Timeout	Timeout for 'call forwarding on no answer' service
SLIC Setting	Impedance matched with analog phone.
REN	The maximum number of extensions that can be connected to a single FXS port. If this parameter is configured, you need to restart the device for the configuration to take effect.
Current Threshold (Off-Hook -> On-Hook, On-Hook -> Off-Hook)	It is used for two conditions. If FXS port connecting with a certain FXS phone, the phone is not under off-hook status, but FXS has detected off-hook. In such condition, users have to set it. If the problem still not be solved, Users may try to set current of off-hook and current of on-hook to 20mA.
Port Current Protection Threshold	Configure the port current anomaly protection threshold, range 0-11, where 0 means off.
Current of Off-Hook (Non-long Line)	Configure current of off-hook, it can be configured with 20, 25, 30, 35, 40mA
Long Line Support	Whether to enable 'Long Analog Extension Line'.

4.12.3 Media Parameter

Media parameters mainly include: RTP start port, DTMF parameter, Preferred Vocoder, etc.

Media Parameter

Use Random Port

☐ Enable

RTP Start Port

12000

UDP Checksum Validation

☒ Enable

SRTP Mode

Disable

DTMF Parameter

DTMF Method

RFC2833

RFC2833 Payload Type Preferred(Incoming Call)

Remote

RFC2833 Payload Type

101

DTMF Gain

0dB

DTMF Send Cadence

100,100

Send Flash Event

☐ Enable

Send DTMF Tone to Analog When Call in Active

☒ Enable

Preferred Vocoder

	Coder Name	Payload Type	Packetization Time(ms)	Rate(kbps)	Silence Suppression
1	G.711U	0	20	64	Disable
2	G.711A	8	20	64	Disable
3	G.729	18	20	8	Disable
4	G.723	4	30	63	Disable
5					

Prefer Codec

Remote

Figure 4.12- 3 Configuration Interface for Media Parameter

Explanation of media parameters:

Use Random Port	If this parameter is enabled, the gateway will choose a port by random as the start port for RTP.
RTP Start Port	Default RTP start port is 8000
UDP Checksum Validation	Choose whether to enable header checksum of UDP
SRTP Mode	Configure whether RTP is encrypted
DTMF Method	Include SINGAL, INBAND and RFC2833
RFC2833 Payload Type Preferred (Incoming Call)	For an incoming call, choose local or remote RFC2833 payload type as the preferred payload type
RFC2833 Payload Type	Local payload value, default value is 101
DTMF Gain	Default value is 0 DB
DTMF Send Cadence	The Send Cadence for sending DTMF signal. The default value is 100,100 (Unit: ms)

Send Flash Event	If this parameter is enabled, the gateway will send flash event to remoteterminal, and thus user does need to handle it locally
Send DTMF Tone to Analog When Call in Active	If this parameter is enabled, DTMF tone will be sent to analog phone when there is a call
Coder Name	The gateway supports G729, G711U, G711A and G723. When outgoing calls are made, G.729 will be used.
Payload Type	Each kind of coding has a unique load value, refer to RFC3551.
Packetization Time	The time for voice packaging
Rate (kbps)	Voice data flow rate; It is defaulted by system.
Silence Suppression	Default value is 'disabled'. If this parameter is enabled, VoIP transmission bandwidth can be saved, and meanwhile network congestion can be avoided.
Prefer Codec	Choose local or remote codec as the preferred codec

4.12.4 Service Parameter

Service parameters include timeout for dialing, digitmap, MWI message and so on.

Service Parameter

Timeout for Off-hook

10

s

Timeout for Dialing

4

s

Timeout for Answer(Outgoing Call)

55

s

Timeout for Answer(Incoming Call)

55

s

No RTP Detected

☐ Enable

Period without RTP Packet

60

s

SUBSCRIBE for MWI(Message Waiting Indicator)

☐ Enable

MWI Subscription Expires(Default: 3600)

3600

s

Voicemail User ID

Visual MWI Type

NEON

▼

NEON Voltage(75-100V)

75

▼

IP-to-IP Call

☐ Enable

Only Accept Calls from ACL(SIP Server or IP Trunk)

☐ Enable

Anonymous Call

☐ Enable

Reject Anonymous Call

☐ Enable

as Ending Dial Key

☒ Enable

Escape

☐ Enable

Send # when First Dial Number is **

☒ Enable

Call Confirm Tone

☐ Enable

Howl Tone Interval After Busytone(0:No Send)

0

s

Max Call Duration(0:No Limit)

0

s

Domain Query Type	A Query
DNS Redundancy Mode	Normal
DNS Cache	☒ Enable
Domain Re-resolution Interval(0-3600,0:No Refresh)	0 s
Echo Cancel Tail	128 ms
Digit Map	
Match Failed(When the registration is successful)	Send to the server
<pre> *x*x*x.*x.# *x*x*x.*x.# *x*x# *#xx# *#60*x.# #x.# #x.*x.# **x.T *11*x.T x.# x.T </pre>	

NOTE: Length of 'Digit Map' should be less than 5120 characters.

Figure 4.12- 4 Configuration Interface for Media Parameters

Explanation of media parameters:

Timeout for off-hook	Mainly used to define a timer that when the user is off hook an analog phone without dial any digits
Timeout for dialing	With the help of dialing timeout, you can limit the time between two digits while users are typing the digits of a number through an extension. If the timeout expires, the gateway will consider the dialing has finished and will try to send message to SIP server. Default value is 4 seconds.
Timeout for answer (Outgoing call)	This parameter determines how long the caller party will wait for answer when making outgoing calls through a phone.
Timeout for answer (Incoming call)	This parameter determines how long the phone rings when there are incoming calls
No RTP Detected	If this parameter is enabled, the situation will be detected when there is no RTP packets received during the set time period.
Period without RTP Packet	The time period when there is no RTP packets received.
SUBSCRIBE for MWI (Message Waiting Indicator)	MWI is aimed to notify user that there is new voicemail. It is realized in the way of NOTIFY.
MWI Subscription Expires	The expiry time of MWI subscription; Default value is 3600s.
Voicemail User ID	The user ID used to access to voicemail
Visual MWI Type	There are two visual MWI Type, namely NEON and FSK

NEON Voltage(75-100V)	Set Voltage for NEON, If the voltage is lower than the value set, the LED will not be in flash.
IP-to-IP Call	If this parameter is enabled, user can dial IP address through a phone to call destination gateway.
Only Accept Call from ACL (SIP server or IP Trunk)	If this parameter is enabled, the device only accepts incoming call from SIP server only. Default value is 'not enable'.
Anonymous Call	If this parameter is enabled, 'anonymous' will be included in SIP message.
Reject Anonymous Call	If this parameter is enabled, all anonymous calls will be rejected. Default value is 'not disable'.
# as ending Dial Key	If this parameter is enabled, '#' is used as the end mark for dialing.
# Escape	If this parameter is enabled, '#' is considered as a digit of the number that is dialed.
Send '#' when First Dial Number is '*'	If this parameter is enabled, '#' will be sent when first dialed digit is '*'.
Call Confirm Tone	If this parameter is enabled, ring-back tone will be played when a call does not receive 180x response.
Howl Tone Interval After Busytone	The time interval for Howler tone after playing Busytone
Max Call Duration	When the duration of call is reach the set time, the call will hang up directly (default is 0, 0 means unlimited)
Domain Query Type	Set the query of the domain name, and support three query methods: A query, SRV query and NAPTR query
DNS Redundancy Mode	Obtain and maintain the DNS SRV list, applicable primarily when the domain query method is SRV/NAPTR, with options to choose between "Basic" and "Advanced".
DNS Cache	When enabled, the device will not initiate domain name query requests to DNS servers during the re-resolution interval.
Domain Re-resolution Interval	Configure the domain name re-resolution interval. The range is 0-3600, and 0 means no refresh
Echo Cancel Tail	Configure echo cancellation duration
Match Failed (When the registration is successful)	Action after failing to match the dialing rule: choose either "Send to the server" or "Call ends"

Voicemail instructions:

Here takes the DAG1000-4S device together with Elastix as the example to introduce how voicemail works in the device.

- (1) After the device registers to Elastix server, enable the voicemail function in Elastix for the corresponding extension number and then set password. As below:

Voicemail & Directory

Status	Enabled
Voicemail Password	111111
Email Address	
Pager Email Address	
Email Attachment	☐ yes ☒ no
Play CID	☐ yes ☒ no
Play Envelope	☐ yes ☒ no
Delete Voicemail	☐ yes ☒ no
IMAP Username	
IMAP Password	
VM Options	
VM Context	default
VmX Locator	

- (2) Check feature code in Elastix and change it if necessary. Its default feature code setting is as follows:

Voicemail

Dial Voicemail	*98	☒	Enabled
My Voicemail	*97	☒	Enabled

- (3) On the Web interface of DAG1000-4S, click **Advanced -> SIP Parameter** in the navigation tree and then enter voicemail User ID.

SUBSCRIBE for MWI(Message Waiting Indicator) ☒ Enable

MWI Subscription Expires(Default: 3600) s

Voicemail User ID

Visual MWI Type

- (4) Set ringing time in Elastix. Elastix will prompt user to leave a message after the corresponding extension rings 15 seconds (by default). Then the Elastix sever will record the message. Related setting is shown as follows:

Voicemail

Ringtime Default:
 Direct Dial Voicemail Prefix:
 Direct Dial to Voicemail message type:
 Optional Voicemail Recording Gain:
 Do Not Play "please leave message after tone" to caller ☐

- (5) Dial *200# on the extension which is connected to DAG1000-4S, and then dial voicemail user ID and password for authentication. After that user will hear voice message.

Digitmap is used for number dialing of calls through FXS ports of the DAG1000-4S device.

Supported Objects	Digit	0-9
	T	Timer
	DTMF	A digit, a timer, or one of the symbols of A, B, C, D, #, or *
Range	[]	One or more DTMF symbols enclosed in the [], but only one DTMF symbol can be selected
Range	()	One or more expressions enclosed the (), but only one can be selected
Separator		Separate expressions or DTMF symbols.
Subrange	-	Two digits separated by hyphen (-) which matches any digit between and including the two digits.
Wildcard	x	Matches any digit of 0 to 9
Modifiers	.	Matches 0 or more times of the preceding element
Modifiers	?	Matches 0 or 1 times of the preceding element

4.12.5 SIP Compatibility

SIP parameters include attended transfer trigger, early media, session timer, heartbeat interval and so on.

SIP Compatibility	
RFC3407 Support	☐ Enable
Forbid "user=phone"	☐ Enable
"From" SIP URI includes "user=phone"	☐ Enable
INVITE with "P-Preferred-Identity" Header (RFC3325)	☐ Enable
Value of "Refer To" refers to "Contact"	☐ Enable
Third Party Do Not Send 18x Response	☐ Enable
REFER Delay	☐ Enable
Send BYE when Recv REFER Response(Unattended)	☐ Enable
Send New REGISTER when Recv 423 Response	☒ Enable
Cseq Start with 1	☐ Enable
Forbid Invalid m=line in reINVITE	☐ Enable
SIP Message with ID Header	MAC
ID Header Separator	None
Call Waiting Response Code	180 Response
RTP Mode in SDP when Call Holding	sendonly
Support Call Waiting of Huawei IPPBX	☐ Enable
Accept Orphan 200 Ok	☐ Enable
Called Number Preferred	P-Called-Party-ID Header
Caller-ID Preferred	P-Asserted-Identity Header
Check SDP Strictly	☒ Enable
Report SDP Whatever	☐ Enable
18x Response Preferred(Without Effective P-Early-Media)	18x Response with SDP
FlashHook Operation Mode	Mode one
Attended Transfer Trigger	Onhook
Multipart Payload Support	☐ Enable
Local Extension is Preferred(Tel in)	☐ Enable
Ignore ACK	☐ Enable
PRACK(RFC3262)	☐ Enable
PRACK Only for 18x with SDP	☐ Enable
Early Media	☒ Enable
Early Answer	☐ Enable
Session Timer(RFC4028)	☐ Enable
Session-Expires	1800 s
Min-SE	1800 s
Session Refresh Method	INVITE
T1	500 ms
T1	500 ms
T2	4000 ms
T4	5000 ms
Max Timeout	32000 ms
Heartbeat Interval(1 - 3600)	10 s
Heartbeat Timeout(4 - (64*T1-1))	16 s
Username of OPTION(Heartbeat) for SIP Server	heartbeat
Username of OPTION(Heartbeat) for IP Trunk	heartbeato
Username of OPTION(Heartbeat) for Switch	activitycheck
Release all call when Heartbeat Timeout	☐ Enable
User-Agent Header	
Response code when Fax Reinvite was Rejected	415

Figure 4.12- 5 SIP Compatibility Configuration Interface

Explanation of SIP Compatibility:

RFC3407 Support	Whether to enable RFC3407 support. If this parameter is enabled, the device will support RFC3407 which defines the SDP capability of backward compatibility.
Forbid "user=phone"	When disabled, the "user=phone" is not carried in the URI
"From" SIP URI Includes "user=phone"	If this parameter is enabled, 'user=phone' will be contained in URI. When calls are routed to PSTN network, the called number will be got from user name. Default value is 'not enable'.
Default Port Display Policy in SIP URL	It supports Hidden, Display and Hide when the host is Domain.
INVITE with "P-Preferred-Identity" Header (RFC3325)	If this parameter is enabled, "P-Preferred-Identity" header will be added in INVITE message for anonymous call (Support RFC3325).
Implicit Subscription	Supports MWI implicit subscription, disabled by default.
Value of "Refer To" refers to "Contact"	If this parameter is enabled, 'contract header' needs to be filled in in the 'refer to' field of a SIP message.
Third Party Do Not Send 18x Response	If this parameter is enabled, the third party will not send 18x response during an attended transfer.
REFER Delay	When the call is in blind transfer status, as a call transfer initiator, it only received a 200 OK from remote side and then send REFER.
Send BYE when Recv REFER Response (Unattended)	If this parameter is enabled, the third party will send BYE to release session after receiving REFER during a blind transfer.
Send New REGISTER when Recv 423 Response	If this parameter is enabled, the value of 'expires' header will be automatically updated and REGISTER will be re-sent after receiving of 423 response.
Verify the Contact Header in REGISTER Response	Enabled it, the contact header will be verified, if the verification failed, the registration will be failed.
Support Wildcard in REGISTER Response	When this parameter is enabled, the device allows wildcard characters in the Contact header of SIP registration responses.

CSeq Start with 1	If this parameter is enabled, the value of CSeq starts with '1'.
Forbid Invalid m=line in reINVITE	If this parameter is enabled, the device will prevent 'invalid m=line' from being carried in the SDP of re-INVITE.
SIP Message with ID Header	SIP header carries two types of IDs with MAC or SN.
ID Header Separator	ID header separator for MAC or SN.
Call Waiting Response Code	User can choose 180 or 182 as call waiting response code
RTP Mode in SDP when Call Holding	Use 'send only' or 'inactive' as RTP mode during call holding.
Support Call Waiting of Huawei IPPBX	If this parameter is enabled, the device will support call waiting of Huawei IPPBX.
Accept Orphan 200 OK	If this parameter is enabled, the DAG3000 device will support different 'to-tag 200 OK' in an INVITE session.
Called Number Preferred	Choose P-Called-Party-ID header or Request-Line
Caller-ID Preferred	Choose P-Asserted-Identity header or From Header
Check SDP Strictly	Strictly or not for SDP check.
Report SDP Whatever	If this parameter is enabled, SDP will be reported anytime
18x Response Preferred	Choose '18x Response with SDP', 'Last 18x Response' or 'Local Ring Tone Only'
Flashhook Operation Mode	Choose Mode one, Mode two or Mode three
Attended Transfer Trigger	Choose 'Onhook' or 'Flashhook +4'
Multiple Flashhook before Attended Transfer	Once enabled, during consultation transfer, a second call is initiated; multiple flashhooks are allowed before initiating the transfer.
Multipart Payload Support	Support MIME types.
Local Extension is Preferred (Tel in)	Once enabled, both locally registered and unregistered ports can make direct calls, and not through the server.
Ignore ACK	If enabled it, When FXS is off-hook, and even though SIP UA does not receive ACK message, the, the device do not resend 200 OK response.

Report Hook State via SIP INFO	If enabled it, whether the FXS is in Off-hook or on-hook status, SIP-INFO will send.
Old Crypto Lable	When enabled, a=crypto uses the old encryption tag for SRTP encrypted calls.
PRACK(RFC3262)	If this parameter is enabled, the DAG3000 device supports reliable transmission of provisional response
PRACK Only for 18x with SDP	If this parameter is enabled, only PRACK will be sent when there's SDP in 18x response
Early Media	If this parameter is enabled, the DAG3000 device supports the receiving of Early Media.
Early Answer	If this parameter is enabled, the DAG3000 device supports early answer
Session Timer (RFC4028)	Whether to enable 'session timer', default value is 'not enable'.
Session-Expires	The interval for refreshing session; default value is 1800s. The Session-Expires header field conveys the session interval for a SIP session.
Min-SE	The minimum interval for refreshing session; default value is 1800s. The Min-SE header field indicates the minimum value for the session interval.
Session Refresh Method	The method to refresh session; default value is INVITE.
T1	Value of T1 timer in SIP protocol, default is 500ms
T2	Value of T2 timer in SIP protocol, default is 4000ms
T4	Value of T4 timer in SIP protocol, default is 5000ms
Max Timeout	The max timeout of sending or receiving SIP messages, default is 32000ms
Heartbeat Interval	The interval for sending heartbeat message, Default is 10s.
Heartbeat Timeout	The timeout for heartbeat message to be sent, default to 16s
Username of OPTION (Heartbeat) for SIP Server	The user ID part of OPTION SIP message in the heartbeat

	request for SIP server
Username of OPTION (Heartbeat) for IP TRUNK	The user ID part of OPTION SIP message in the heartbeat request for IP trunk
Username of REGISTER (Connectivity Check)	The gateway uses the user ID field in REGISTER requests to verify connectivity with the SIP server. By regularly sending REGISTER requests, it confirms the server's reachability and status, ensuring the validity of registration information and the proper establishment of sessions.
Release all call when Heatbeat Timeout	If enabled, when the heartbeat times out, all calls will be disconnected
User-Agent Header	Customize User-Agent header field value
Response code when Fax Reinvite was Rejected	Customize the SIP response code when fax re-invite was rejected

4.12.6 NAT Parameter

NAT Traversal (Network Address Translator Traversal) is a computer networking technique of establishing and maintaining Internet protocol connections across gateways that implement network address translation (NAT). NAT breaks the principle of end-to-end connectivity originally envisioned in the design of the Internet.

STUN (Simple Traversal of UDP over NATs) is a lightweight protocol that allows applications to discover the presence and types of NATs and firewalls between them and the public Internet. It also provides the ability for applications to determine the IP addresses allocated to them by the NAT. STUN works with many existing NATs, and does not require any special behavior from them. STUN doesn't support TCP connection and H.323.

Static NAT: Uses a fixed NAT address.

Dynamic NAT: The gateway detects the NAT address via the rport method.

DTR: Employs proprietary technology to resolve penetration issues in complex network environments, supporting automatic detection and enabling forwarding functions.

NAT Config

NAT Traversal

Via of Message

Contact of Message

SDP of Message

Dynamic NAT ▼

☒ Local Address

☐ Local Address

☒ Local Address

☐ NAT Address

☒ NAT Address

☐ NAT Address

Figure 4.12- 6 NAT Parameter

Explanation of NAT Parameters:

NAT Traversal	Supports four NAT traversal methods: STUN, Static NAT, Dynamic NAT, DTR.
NAT IP	When Static NAT is selected for NAT traversal, configure a fixed NAT address.
Refresh interval	When STUN is selected for NAT traversal, periodically query the NAT address.
STUN Server Address	Configure the STUN server IP address, supporting both IP and domain names.
STUN Server Port	Configure the STUN server port.
Via of Message	Use local address or NAT address in the Via header of SIP messages
Contact of Message	Use local address or NAT address in the Contact header of SIP messages
SDP of Message	Use local address or NAT address in the SDP carried by SIP messages

4.12.7 Speed Dial

Speed dial is a function that is available on telephones which provides an easy method of calling a telephone number by pressing fewer digits on the keypad. The tool enables one to save, organize, and have easy and quick access to regularly dialed numbers.

Speed Dial		
Index	Speed Dial Number	Original Number
---	---	---

59

User Manual

Shenzhen Dinstar Co.,Ltd.

 www.dinstar.com

Speed Dial - Add

Index

0

Speed Dial Number

10

Original Number

888123

Speed Dial			
	Index	Speed Dial Number	Original Number
☐	0	10	888123

Total: 1 Entry

Figure 4.12- 7 Add Speed Dial

4.12.8 Feature Codes

Feature Code			
Feature	Codes	Use Default	Status
Device Function			
Inquiry LAN IP	*158#	☒	Enable v
Inquiry WAN IP	*159#	☒	Enable v
Inquiry Phone Number	*114#	☒	Enable v
Inquiry PortGroup Number	*115#	☒	Enable v
Inquiry Registration Status	*168#	☒	Enable v
Remove Login Limit	*154#	☒	Enable v
Setting IP Mode	*150*	☒	Enable v
Network Work Mode	*157*	☒	Enable v
Configure IP Address	*152*	☒	Enable v
Network Subnet Mask Configure	*153*	☒	Enable v
Network Gateway Configure	*156*	☒	Enable v
Port Voice Up	*170#	☒	Enable v
Port Voice Down	*171#	☒	Enable v

Access by WAN in Route Mode	*160*	☒	Enable ▼
Reset Basic Configuration	*165*	☒	Enable ▼
Reset Factory Configuration	*166*	☒	Enable ▼
Restart Device	*111#	☒	Enable ▼
Call Function			
Call by IP	*47*	☒	Enable ▼
Call Waiting Activate	*51#	☒	Enable ▼
Call Waiting Deactivate	*50#	☒	Enable ▼
Blind Transfer	*87*	☒	Enable ▼
Call Forward Unconditional Activate	*72*	☒	Enable ▼
Call Forward Unconditional Deactivate	*73#	☒	Enable ▼
Call Forward Busy Activate	*90*	☒	Enable ▼
Call Forward Busy Deactivate	*91#	☒	Enable ▼
Call Forward No Reply Activate	*92*	☒	Enable ▼
Call Forward No Reply Deactivate	*93#	☒	Enable ▼
Do Not Disturb Activate	*78#	☒	Enable ▼
Do Not Disturb Deactivate	*79#	☒	Enable ▼
Dial Voicemail	*200#	☒	Enable ▼
DTMF Function			
Call Holding	*#	☒	Enable ▼
Call Switch	##	☒	Enable ▼

Figure 4.12- 8 Feature Codes

Explanation of Feature Code

Inquiry LAN IP	Dial*158# to obtain device WAN port IP address
Inquiry WAN IP	Dial*159# to obtain device WAN port IP address
Inquiry Phone Number	Dial*114# to obtain port account
Inquiry PortGroup Number	Dial *115# to obtain port group number
Inquiry Registration Status	Dial *168# to obtain port registration status
Remove Login Limit	Dial *154# to remove login limit
Setting IP Mode	*150*0#, means pppmodem, *150*1#, means static IP, *150*2#,means obtain IP address by DHCP, *150*3#, means pppoe.
Network Work Mode	*157*0#, set network work mode to routing mode; *157*1#, setnetwork work mode to bridge mode

Configure IP Address	*152*+IP, set gateway IP address
Network subnet mask configure	*153*+subnet mask, set gateway subnet mask
Network Gateway Configure	*156*+gateway IP, set gateway
Port Voice Up	Please dial "**170#" to increase the port VOL Only when the port choosing the Tel Profile, then apply to the Tel Profile.
Port Voice Down	Please dial "**171#" to reduce the port VOL Only when the port choosing the Tel Profile, then apply to the Tel Profile.
Reset Basic Configuration	Dial *165*000000# to restore default username/password and networkconfiguration
Reset Factory Configuration	*166*000000#, reset factory
Restart Device	*111#, restart device
Call by IP	Directly dial the end user IP to call
Call Waiting Activate	*51#, enable call waiting function
Call Waiting Deactivate	*50#, forbid call waiting function
Blind Transfer	If the call transfer to 801, first hook flash and then dial the * 87 * 801#
Call Forward Unconditional Activate	*72*+ phone number#, transfer the call from the phone number
Call Forward Unconditional Deactivate	*73#, forbid call forward unconditional
Call Forward Busy Activate	*90*+ forward busy number#
Call Forward Busy Deactivate	*91#, forbid call forward busy
Call Forward No Reply Activate	*92*+ forward no reply number#
Call Forward No Reply Deactivate	*93#, close this function
Do Not Disturb Activate	*78#, enable DND function
Do Not Disturb Deactivate	*79#, close DND function

Dial Voicemail	*200#, visit voice mail box
Call holding	During a call, dial *# in 2s to hold the call. (back the call by hook flash or dialing *#)
Call Switch	When the port has two calls, if dial ##, release the current call and restore the inactive call.

4.12.9 System Parameter

System parameters include NTP, daylight saving time, web parameter, telnet parameter and remote management. NTP (Network Time Protocol) is a computer time synchronization protocol.

System Parameter	
Hint Language	English ▼
NTP	
☒ Enable	
Primary NTP Server Address	0.pool.ntp.org
Primary NTP Server Port	123
Secondary NTP Server Address	1.pool.ntp.org
Secondary NTP Server Port	123
SYN Interval	3600 s
Time Zone	GMT+8:00 (Beijing, Singapore, Taipei, ▼)
Local Time	9/15/2025, 2:19:53 PM Sync
Daylight Saving Time	☐ Enable
Log	
Summary	☐ Enable
System Log	☐ Enable
Network Diagnose	
The local network fault detection (Please close for network disable ping)	☐ Enable
The local network interruption detection	☐ Enable
WEB Parameter	
HTTP Enable	☒ Enable
WEB Port	80
HTTPS Enable	☒ Enable
SSL Port	443
No operation logout time(0: No Limit)	5 Minute
Maximum number of consecutive failed login attempts	5
Continuous login failure lock time(0: Always locked)	30 Minute
HTTP HOST Checking	☒ Enable
HTTP X Frame Options	☒ Enable
Strict-Transport-Security	☒ Enable
HTTP REFERER Checking	☒ Enable
Telnet Parameter	
Telnet Enable	☒ Enable
Telnet Port	23
SSH Parameter	
SSH Enable	☒ Enable
Remote Management	
Access WEB by WAN	☒ Enable
Access WEB by LAN	☒ Enable
Access Telnet by WAN	☒ Enable
Access Telnet by LAN	☒ Enable

Figure 4.12- 9 Configuration Interface for System Parameter

Explanation for related parameters:

NTP	To Enable or disable NTP
Primary NTP server address	The IP address of primary NTP server, default IP address is us.pool.ntp.org.
Primary NTP server port	The service port of primary NTP server. Default port is 123.
Secondary NTP server address	The IP address of secondary NTP server, Default IP address is 64.236.96.53
Secondary NTP server port	The service port of secondary NTP server. Default port is 123
SYN Interval	The interval to synchronize the time of the DAG1000-4S. Default value is 3600s.
Time Zone	The time zone of the gateway, Default configuration is United States central time, Chicago.
Local time	Enable or disable daylight saving time
Daylight Saving Time	Enable or disable daylight saving time
Periodic Self-Checking	Enable or disable periodic self-checking
Summary	Record detailed call logs and save them to a summary log file
System Log	Save critical logs during device operation to the summary log file.
The local network fault detection (Please close for network disable ping)	Select whether to enable local network fault detection. If local network Ping is disabled, this option must be turned off.
The local network interruption detection	Enable or disable local network interruption detection
Http Enable	Enable the device's HTTP web service and allow HTTP protocol access to the device management interface, default is disable.
WEB Port	The web port of the gateway. Default port is 80
Https Enable	Enable HTTPS for secure web access. Once enabled, the management interface uses an encrypted connection for enhanced security.
SSL Port	The SSL port. Default is 443

No operation logout time	After logging into the user management interface, the system will automatically log out if there is no activity within the set time. A value of 0 means no automatic logout.
Maximum number of consecutive failed login attempts	The number of incorrect login attempts allowed before further attempts are blocked to prevent brute-force attacks.
Continuous login failure lock time	The duration of the login block after reaching the maximum failed attempts. A value of 0 means permanent lockout.
HTTP HOST Checking	When enabled, checks the Host field in the HTTP request header to ensure the Host value matches the device's IP address. Requests are rejected if there is no match.
HTTP X Frame Options	When enabled, adds the X-Frame-Options header to HTTP responses to control whether the page can be embedded within an <iframe>.
Strict-Transport-Security	When enabled, sends the Strict-Transport-Security HTTP response header to the client, instructing the browser to communicate with the device exclusively over HTTPS for a specified period.
HTTP REFERER Checking	When enabled, checks the Referer field in the HTTP request header to verify that the request originates from a page belonging to the device's IP address.
Telnet Enable	Choose whether to enable the Telnet service, default is disable.
Telnet port	Listening port of telnet service; Default port is 23
SSH Enable	Choose whether to enable the SSH service.
Access WEB by WAN	Enable or disable 'web service from WAN'
Access WEB by LAN	Enable or disable 'web service from LAN'
Access Telnet by WAN	Enable or disable 'telnet service from WAN'
Access Telnet by LAN	Enable or disable 'telnet web service from LAN'

Note:

After Web port and Telnet port are configured, please restart the device for the configurations to take effect.

4.13 Call & Routing

4.13.1 Wildcard Group

A wildcard group IMPU is a registration method that associates multiple ports under a single port when network traffic is heavy. A single wildcard group IMPU can represent multiple physical users, avoiding individual registrations for each user and reducing signaling overhead. This requires IMS integration for wildcard IMPU registration.

One or more SIP accounts from the account pool composed of all non-wildcard IMPU SIP accounts are left-shifted to become associated IMPUs. After adding the wildcard group, the device uses the wildcard IMPU to initiate registration, with both the From and To header fields set to the wildcard IMPU. Upon successful registration, the 200 OK response's P-Associated-URI contains a wildcard-formatted number. Checking the port status in status and statistics shows that both the wildcard IMPU and associated IMPUs are in a registered state.

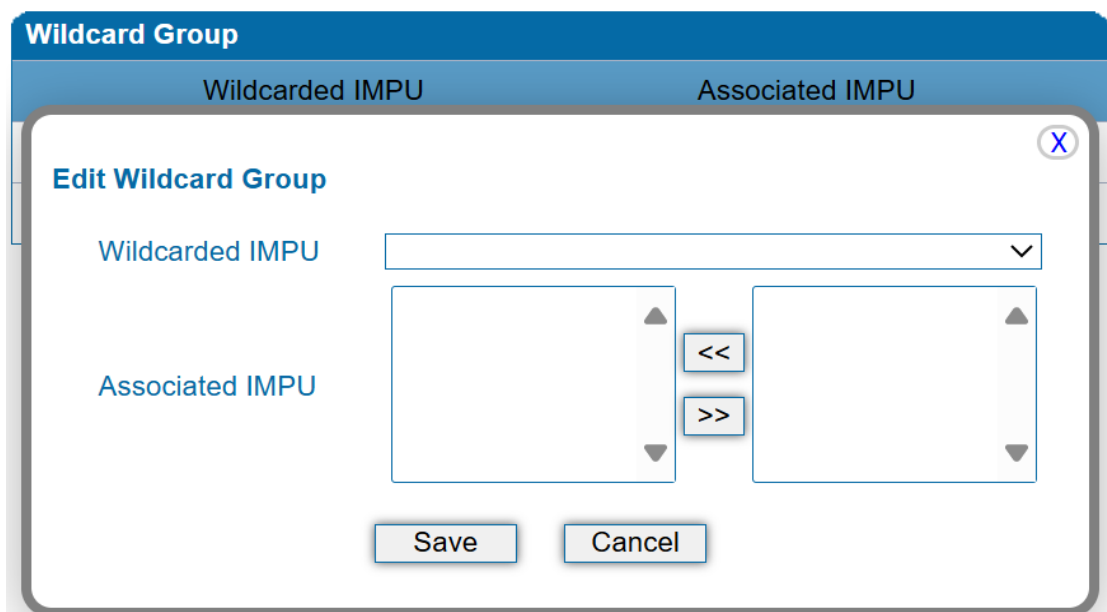


Figure 4.13- 1 Wildcard Group

4.13.2 Port Group

On the **Port Group** interface, user can group several ports together and then set a strategy for port selection of the group. Parameters of port group include registration, display name, SIP user id, authentication ID and password, off-hook auto dial, auto dial delay time, port select and so on.

Port Group Add

Index
3

Registration
☒ Enable

IP Profile
0 <default>

Description

Display Name

SIP User ID

Authenticate ID

Authenticate Password

Offhook Auto-Dial

Auto-Dial Delay Time
s

Port Select
Cyclic Ascending

Pick Up on Group
*#

Select Port Count
Cyclic Select

Port
Select Port for this Group

Figure 4.13- 2 Configuration Interface for Port group

Explanation of Port Group parameters

Index	The NO. of the port group, it uniquely identifies a route
Registration	Check if the port requires registration
IP Profile	Select the IP Profile from the dropdown as needed; the default IP Profile is generally used.
Description	The description of the port group; it is used to identify the port group
Display Name	Display name of the port group, which will be used in SIP message, for example: INVITE sip: bob@biloxi.com SIP/2.0 Via: SIP/2.0/UDPpc33.atlanta.com;branch=z9hG4bK776asdhds Max-Forwards: 70 To: Bob <sip:bob@biloxi.com> From: Alice <sip:alice@atlanta.com>;tag=1928301774 Here Bob and Alice is the display name
SIP User ID	User ID of this SIP account, which is provided by VoIP service provider (ITSP). Usually in the form of digit similar to phone number or an actual phone number.
Authenticate ID	SIP service subscriber's authentication ID, it can be identical to or different from SIP User ID.

Authenticate Password	SIP service subscriber's password for authentication
Offhook Auto-Dial	An extension or phone number is pre-assigned here so that the number is automatically dialed as soon as user picks up the phone
Auto-dial Delay time	How long auto-dialing will be delayed
Port Select	It specifies the policy for selecting a port for ringing in the port group • Ascending: the gateway always selects a port from the minimum number. • Cyclic ascending: the gateway always selects a port from a number next to the number selected last time. If the maximum number was selected last time, the next selected number is the minimum number. The sequence moves in cycles like this. • Descending: the gateway always selects a port from the maximum number. • Cyclic descending: the gateway always selects a port from a number next to the number selected last time. If the minimum number was selected last time, the next selected number is the maximum number. The sequence moves in cycles like this. • Group ring: all ports ring at the same time
Pickup UP on group	When one port rings, user can dial “*#” to pick up the call from other ports under the same port group.
Select Port Count	Support Port Count: Cyclic Select and Only Once
Port	Select ports for this port group

4.13.3 IP Trunk

A peer-to-peer VoIP call occurs when two VoIP phones communicate directly over IP network without IP PBXs between them. IP trunk helps establish peer-to-peer call between gateway and VoIP phones. IP trunk will be used in routing configuration.

IP Trunk Add

Index

94

▼

IP Profile

0 <default>

▼

Description

Remote Address

Remote Port

Heartbeat

☐
Enable

Figure 4.13- 3 IP Trunk Configuration Interface

Explanation of IP Trunks parameters:

Index	The No. of the IP trunk
Description	The description of the IP trunk; It is used to n identify the IP trunk
Remote Address	IP address or domain name of peer device
Remote Port	SIP port of peer device
Heartbeat	Whether to enable the 'Heartbeat' function for the IP trunk. Default value is 'disable'. If heartbeat is enabled, the gateway will send "OPTION" to peer device.

4.13.4 Routing Parameter

This parameter determines a call is routed before or after manipulation.

Routing Parameter

Calls from IP

Routing before Manipulation

▼

Calls from Analog Line

Routing before Manipulation

▼

Figure 4.13- 4 Configuration Interface for Routing Parameter

Explanation of Routing Parameters:

Calls from IP	Choose calls from IP network are routed before manipulation or after manipulation.
Calls from Analog Line	Choose calls from analog lines are routed before manipulation

	or after manipulation.
--	------------------------

4.13.5 IP -> Tel Routing

Calls from IP network can be routed to FXS port or port group of the DAG1000-4S device through IP ->Tel routing.

IP->Tel Routing Add

Index	127	
Description		
Calls from	☐ IP Trunk	Any
	☒ IP Profile	0 <default>
Caller Prefix		
Called Prefix		
Calls to	☐ Port	1
	☒ Port Group	7 <1058190001>

Figure 4.13- 5 IP-Tel Routing

Explanation of IP -> Tel Routing Parameters:

Index	IP ->Tel Routing priority: from 0 to127, 0 is the highest priority.
Description	Description of the IP -> Tel routing. It is used to identify the IP -> Tel routing.
Calls from	Choose calls from IP Trunk or SIP Server, 'any' means any IP addresses.
Caller Prefix	The prefix of the caller number, which helps match routing exactly. its length is less than or equal to the caller number. For example, if caller number is 2001, the caller prefix can be 200 or 2. 'any' means the prefix matches any caller number.
Callee Prefix	The prefix of the called number, which helps match routing exactly. Its length is less than or equal to the called number. If the called number is 008675526456659, the called prefix can be 0086755 or 00., "any" means the prefix matches any called number.
Calls to	Which port or port group to which calls are routed.

4.13.6 Tel->IP/Tel Routing

Tel->IP/Tel Routing Add	
Index	126
Description	
Calls from	☒ Port 1 ☐ Port Group 7 <1058190001>
Caller Prefix	
Called Prefix	
Calls to	☐ Port 1 ☐ Port Group 7 <1058190001> ☐ IP Trunk ☒ IP Profile 0 <default>

Figure 4.13- 6 Tel->IP/Tel Routing

Explanation of Tel->IP/Tel Routing parameters:

Index	The index of this Tel->IP/Tel routing, from 0 to 127. Each index cannot be used repeatedly. Routing priority: 0 is the highest priority.
Description	It is used to identify the routing
Calls From	Tel->IP/Tel calls are from a port or a port group
Caller Prefix	The prefix of the caller number, which helps match routing exactly. its length is less than or equal to the caller number. For example, if caller number is 2001, the caller prefix can be 200 or 2. 'any' means the prefix matches any caller number.
Callee Prefix	The prefix of the called number, which helps match routing exactly. Its length is less than or equal to the called number. If the called number is 008675526456659, the called prefix can be 0086755 or 00., "any" means the prefix matches any called number.
Calls to	Calls are routed to a port, port group, IP trunk or SIP server

4.14 Manipulation

Number manipulation refers to the change of a called number or a caller number during calling process when the called number or the caller number matches the preset rules.

4.14.1 IP -> Tel Called

IP->Tel Called Add

Index	127 ▼
Description	
Calls from	☐ IP Trunk Any ▼ ☐ IP Profile 0 <default> ▼
Caller Prefix	
Called Prefix	
Calls to	☒ Port 1 ▼ ☐ Port Group 7 <10581900 ▼
Stripped Digits from Left	
Stripped Digits from Right	
Prefix to Add	
Suffix to Add	
Number of Digits to Leave from Right	

Figure 4.14- 1 Add IP -> IP Called Number Manipulation

Explanation of IP->Tel Called Number Manipulation Parameters:

Index	The index of this manipulation, from 0 to 127. Each index cannot be used repeatedly. 0 is the highest priority
Description	Name of this IP ->Tel manipulation name
Calls From	Determine the calls come from IP trunk or SIP server
Caller Prefix	Set a prefix for caller number. The prefix's length is less than or equal to that of the caller number, which helps to match routing. If caller number is 2001, the caller prefix can be 200 or 2. "any" means match any caller number.
Called Prefix	Set a prefix for called number. The prefix's length is less than or equal to called number, which helps to match routing. If called number is 008675526456659, the called prefix can be 0086755 or 00., "any" means match any called number
Calls to	Determine the port or port group to which the call is routed.
Stripped Digits from Left	The number of digits which are lessened from the left of the called number
Stripped Digits from Right	The number of digits which are lessened from the right of the called number.
Prefix to Add	The prefix added to the called number after its digits are lessened.

Suffix to Add	The suffix added to the called number after its digits are lessened.
Number of Digits to Leave from Right	The number of the retained digits which. are counted from the right of the called number

4.14.2 Tel -> IP/Tel Caller

Tel->IP/Tel Caller Add

Index	127
Description	
Calls from	☒ Port 1 ☐ Port Group 7 <10581900
Caller Prefix	
Called Prefix	
Calls to	☐ Port 1 ☐ Port Group 7 <10581900 ☐ IP Trunk Any ☐ IP Profile 0 <default>
Stripped Digits from Left	
Stripped Digits from Right	
Prefix to Add	
Suffix to Add	
Number of Digits to Leave from Right	

Figure 4.14- 2 Add Tel -> IP/Tel Caller Number Manipulation

Explanation of Tel->IP/Tel Caller Number Manipulation Parameters:

Index	The index of this manipulation, from 0 to 127. Each index cannot be used repeatedly. 0 is the highest priority
Description	Name of this Tel -> IP/Tel manipulation name
Calls From	Determine the calls come from a port or a port group
Caller Prefix	Set a prefix for caller number. The prefix's length is less than or equal to that of the caller number, which helps to match routing. If caller number is 2001, the caller prefix can be 200 or 2. "any" means match any caller number.
Called Prefix	Set a prefix for called number. The prefix's length is less than or equal to called number, which helps to match routing. If called number is 008675526456659, the called prefix can be 0086755 or 00., "any" means match any called number

Calls to	Determine the call is routed to a port, a port group, an IP trunk or a SIP server.
Stripped Digits from Left	The number of digits which are lessened from the left of the calleenumber
Stripped Digits from Right	The number of digits which are lessened from the right of the caller number
Prefix to Add	The prefix added to the caller number after its digits are lessened.
Suffix to Add	The suffix added to the caller number after its digits are lessened.
Number of Digits to Leave from Right	The number of the retained digits which. are counted from the right ofthe caller number

4.14.3 Tel-IP/Tel Called

Tel->IP/Tel Called Add

Index	127 ▼
Description	
Calls from	☒ Port 1 ▼ ☐ Port Group 7 <10581900C ▼
Caller Prefix	
Called Prefix	
Calls to	☐ Port 1 ▼ ☐ Port Group 7 <10581900C ▼ ☐ IP Trunk Any ▼ ☐ IP Profile 0 <default> ▼
Stripped Digits from Left	
Stripped Digits from Right	
Prefix to Add	
Suffix to Add	
Number of Digits to Leave from Right	

Figure 4.14- 3 Add Tel->IP/Tel Called Number Manipulation

Explanation of Tel->IP/Tel Called Number Manipulation Parameters:

Index	The index of this manipulation, from 0 to 127. Each index cannot be used repeatedly. 0 is the highest priority
Description	Description of this manipulation; it is used to identify this manipulation.
Calls From	Determine the calls come from a port or a port group
Caller Prefix	Set a prefix for caller number. The prefix's length is less than or equal to that of the caller number, which helps to match routing. If caller number is 2001, the caller prefix can be 200 or 2. "any" means match any caller number.
Called Prefix	Set a prefix for called number. The prefix's length is less than or equal to called number, which helps to match routing. If called number is 008675526456659, the called prefix can be 0086755 or 00., "any" means match any called number
Calls to	Determine the call is routed to a port, a port group, an IP trunk or a SIP server.

Stripped Digits from Left	The number of digits which are lessened from the left of the called number
Stripped Digits from Right	The number of digits which are lessened from the right of the called number
Prefix to Add	The prefix added to the called number after its digits are lessened.
Suffix to Add	The suffix added to the called number after its digits are lessened.
Number of Digits to Leave from Right	The number of the retained digits which. are counted from the right of the called number

4.15 Routing rule examples

4.15.1 Route any calls from any IP to specific port

After enter the Web interface, click **Call & Routing -> IP-Tel Routing** in the navigation tree on the left, and then click **Add** to create a new routing rule.

IP->Tel Routing Add

Index

127

Description

any

Calls from

☒ IP Trunk

Any

☐ IP Profile

0 <default>

Caller Prefix

any

Called Prefix

any

Calls to

☒ Port

1

☐ Port Group

7 <1058190001>

Save

Reset

Cancel

NOTES: 'any' in 'Called Prefix' or 'Caller Prefix' means wildcard string.

In the example above, all calls will be routed to port 1 when the routing rule is matched.

4.15.2 Route any calls from any IP to specified port group

- Create port group

Before we can route calls to a port group, create the port group first as below. On the **Call & Routing -> Port Group**, click **Add** to create a new port group.

- ✓ Port 1 to port 2 are assigned to port group
- Route any calls to the port group

On the **Call & Routing -> IP-Tel Routing** interface, click **Add** to create a new routing rule.

NOTES: 'any' in 'Called Prefix' or 'Caller Prefix' means wildcard string.

- ✓ As shown above, if the routing rule is matched, calls will be routed to port group 7.

4.15.3 Route any calls from any port to specific SIP IP trunk

Create IP Trunk on the **Call & Routing -> IP Trunk** interface:

IP Trunk Add

Index	31
IP Profile	0 <default>
Description	To_Elastix
Remote Address	172.16.125.125
Remote Port	5060
Heartbeat	☐ Enable

After IP Trunk is created, check the following configuration:

IP Trunk					
	Index	Description	Remote Address	Remote Port	Heartbeat
☐	31	To_Elastix	172.16.125.125...	5060	Disable

Total: 1 Entry Page 1 v

Add
Modify
Delete

As shown above, the IP trunk is created, and the remote end IP address is 172.16.125.125, the SIP port is 5060.

Create Tel -> IP routing rule

On the **Call & Routing -> Tel-IP Routing** interface, click “Add” to create a new Tel -> IP routing rule.

Tel->IP/Tel Routing Add

Index	126
Description	Tel-IPTrunk
Calls from	☒ Port Any
	☐ Port Group / <123>
Caller Prefix	any
Called Prefix	any
Calls to	☐ Port 1
	☐ Port Group 7 <123>
	☒ IP Trunk 311 <To_Elastix>
	☐ IP Profile 0 <default>

All Tel calls from any caller number to any called number will be routed to IP trunk 311.

4.16 Maintenance

4.16.1 TR069

TR069 is short for Technical Report 069, which provides a commonly-used framework and protocol for next-generation network devices. As an application-level protocol on top of IP TR069 has no limitation to access ways of network devices.

Under the network management model of TR069, ACS (Auto-Configuration Server) works as a management server, responsible for managing CPEs (Custom Premise Equipment).

ACS URL (auto-configuration server URL address) is provided by service provider. ACS URL generally starts with http:// or https://

Username and password are used for ACS authentication.

Figure 4.16- 1 TR069 Parameters

Explanation of TR069 Parameters:

TR069	Choose whether to enable TR069; it is 'not enable' by default.
ACS URL	The IP address or domain name of ACS, which is provided by service provider.
User Name (ACS)	Username of ACS, which is provided by service provider.
Password (ACS)	Password of ACS, which is provided by service provider.
Periodic Inform	Choose whether to enable 'Periodic Inform'; if it is enabled, ACS will connect to CPE every 30 seconds (if the interval is set as 30 seconds).
Periodic Inform Interval	The interval set for periodic connection between ACS and CPE.

Username (CPE)	Username of CPE
Password (CPE)	Password of CPE
Port	The port to connect CPE and ACS

4.16.2 SNMP

SNMP (Simple Network Management Protocol) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.

SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

Three significant versions of SNMP have been released. SNMPv1 is the original version of the protocol. More recent versions, SNMPv2c and SNMPv3, feature improvements in performance, flexibility and security.

SNMP Parameter

Snmpp

☐ Enable

Snmpp Version

v1

Community Configuration

	Community	Source
1		
2		
3		

Note: Value of Source is default or IP Address(eg:192.168.1.1)!

Group Configuration

	Group	Community
1		
2		
3		

View Configuration

	ViewName	ViewType	ViewSubtree	ViewMask
1				
2				
3				

Note: Value style of ViewSubtree is x.x.x.x.x(multi-nodes) or .x(one node).

Access Configuration

	Group	Read	Write	Notify
1				
2				
3				

Note: The value of Read/Write/Notify references to ViewName in View Configuration.Access Configuration is base on Group Configuration and View Configuration.

Trap Configuration

	Trap Type	Trap IP	Trap Port	Trap Community
1			0	

Figure 4.16- 2 SNMP Parameters

Explanation of TR069 Parameters:

SNMP	The DAG1000-4S device supports three versions of SNMP, namelyV1、 V2C and V3.
Community Configuration	Community configuration exists in V1 and V2C. Community: fill in a community name used to read through SNMP protocol; it is a character string. Source: The IP address of SNMP server. SNMP server cannot identify the packets sent from DAG1000-4S

	unless the community configured in DAG1000-4S matches with the community configured in SNMP server.
Group Configuration	Group configuration exists in V1 and V2C and V3. Group: fill in a group name which is used to identify the group; it's a character string. Community: fill in a community which means this community has joined in the group. In the following, access permission of read, write and notify is configured for each group.
View Configuration	View configuration exists in V1, V2C and V3. ViewName: fill in a view name which is used to identify this view. ViewType: choose 'Included' or 'Excluded'. 'Included' means the view includes the OID of the corresponding ViewSubtree, while 'Excluded' means the OID of the corresponding ViewSubtree is excluded from this view. ViewSubtree: fill in the OID of the view subtree. ViewMask: it is used to withdraw a row of a table, such as an Ethernet port.
Access Configuration	Access configuration exists in V1, V2C and V3, under which permission of read, write or notify is configured for a community group. Group: choose a group name that has been configured. Read: Choose a 'read' view for the group. Write: Choose a 'write' view for the group. Notify: Choose a 'notify' view for the group.
Trap Configuration	Trap configuration exists in V1, V2C and V3, which is aimed to send trap alarm. Trap Type: Choose V1, V2C and Inform. Trap IP: the IP address of the destination SNMP server where trap alarm is sent. Trap Port: the port of the destination SNMP server, which will receive trap alarm. Trap Community: the community configured in the destination SNMP server.
User Configuration	User configuration exists in V3. When V3 transmits SNMP packets in an encryption way, this item needs to be configured. User: fill in a user name used to authenticate. AuthType: choose MD5 or SHA as authentication type. AuthPassword: the password used to authenticate.

	Privacy Type: Choose DES, AES or AES 128 as encryption type. Privacy Password: the encryption password.
--	--

4.16.3 Syslog

Syslog is a standard for network device data logging. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices which would otherwise be unable to communicate a means to notify administrators of problems or performance.

Syslog levels include: EMERG, ALERT, CRIT, ERROR, WARNING, NOTICE, INFO and DEBUG.

The Signal Log is include following traces which defined in system by default

Syslog

Local Syslog

☐ Enable

Server Address

Server Port

Syslog Level

CDR

☒ Enable

Signal Log

☐ Enable

Media Log

☐ Enable

System Log

☐ Enable

Management Log

☐ Enable

Figure 4.16- 3 Syslog Parameter

Enable send CDR, and then send communication information to syslog server.

When the DAG1000-4S device registers to SIM Cloud server, local syslog will be changed to non-configurable and all logs will be stored on the Cloud server.

4.16.4 Provision

Provision is used to make the DAG1000-4S automatically upgrade with the latest firmware stored onan http server an ftp server or a tftp server.

Provision

Basic Configuration

URL

Check Interval

Account

Password

Proxy Domain

Proxy Port

Proxy Account

Proxy Password

Figure 4.16- 4 Provision

Explanation of Provision Parameters:

URL	Provisioning server URL, support HTTP, TFTP, FTP
Check Interval	The interval to check the changes on the provisioning server
Account	Account for login provisioning server
Password	Account for login provisioning server

4.16.5 User Manage

On the **Management -> User Manage** page, the administrator of the DAG1000-4S device can classify users in different groups, and set login username and password for each user.

Add a User

User Name

Group

Enabled

Password

Confirm Password

Figure 4.16- 5 User Manage

Explanation of Adding a User:

Username	Username
Group	Support User and Guest
Enabled	Enabled
Password	Password
Confirm Password	Confirm password

Note:

The password cannot be less than 8 characters and must contain the following four types of characters: uppercase letters, lowercase letters, numbers, and characters

4.16.6 Radius Parameter

After the Radius server is configured, you can log into the gateway after successful Radius authentication. The Radius server configuration page is shown in Figure:

Figure 4.16- 6 Radius Parameter

Explanation of Radius Parameters:

Radius	Enable or disable Radius
Local Port	The port of the local Radius client
Device Behavior Upon RADIUS Timeout	Processing after Radius authentication timeout. Verify Access Locally: After the timeout, when verifying the user name and password of the local Web login is successful, the login is successful; Deny Access: No matter what, the login is refused
Server IP	The IP address of the Radius server
Server Auth Port	The port of the Radius server
Server Key	The key of the Radius server

4.16.7 Action URL

Action URL is a means of allowing VoIP platform/VoIP server to learn about the statuses of the DAG1000-4S device. This is realized by GET request over the HTTP protocol. During the transmission of status, some data (such as device ID, mac address, called/caller number, IP address) carried in GET request can also be reported to VoIP platform/VoIP server.

The data that can be carried in GET request, please refer to the notes on the **Management -> Action URL** page.

Action URL Configuration	
Event	Action URI
Startup	
Offhook	
Onhook	
Incoming Call	
Outgoing Call	
Call Build	
Call Terminate	
Register Status	
Heartbeat	
Heartbeat Interval	10 s

Figure 4.16- 7 Action URL

Event: Statuses of DAG1000-4S device, which will be reported to VoIP platform/VoIP server.

Action URL: for example, [http://host:port/file.php?macaddr=\\$mac](http://host:port/file.php?macaddr=$mac), among which 'host' means the HTTP server's IP address or domain name, 'port' means the http server's listening port, 'file.php' means the script that will process this request, and '\$mac' means the parameter carried in the request when this request is sent out.

Heartbeat: heartbeat packets are sent to URL by the DAG1000-4S device, used to examine the connection between the DAG1000-4S device and HTTP/HTTP server.

4.16.8 SIP PNP

The gateway can restore the profile and upgrade the software version through SIP PNP. The SIP PNP process is as follows:

- 1) The gateway sends request packet for SIP subscription to the multicast at intervals
- 2) The gateway receives the Notify message and reads the URL address of the deployment server in the message
- 3) Initiate the Provision to the URL to restore the profile or upgrade the software version

SIP PNP	
PNP Enable	☒
Server Address	224.0.1.75
Server Port	5060
Update Interval	3600 s

Figure 4.16- 8 SIP PNP

Explanation of SIP PNP Parameters:

PNP Enable	Enable or disable PNP
-------------------	-----------------------

Server Address	SIP PNP server IP address, and the default is the multicast address 224.0.1.75
Server Port	SIP PNP server port, and the default is 5060
Update Interval	Send subscription messages periodically, and 3600s by default

4.16.9 NMS

NMS is a public/private cloud-based device management platform. After users register with the NMS, you can perform batch upgrades, status monitoring, and view alarm information for the devices. To apply for cloud management server (NMS), please contact your local distributor.

NMS Configuration

NMS Enable

☒ Enable

NMS Address

NMS Port

0

Figure 4.16- 9 NMS Configuration

Explanation of NMS Parameters:

NMS Enable	Enable or disable NMS
NMS Address	IP address or domain address of the NMS server
NMS Port	Port of the NMS server, the default is 0

4.16.10 TACACS Parameter

TACACS is a protocol for user authentication and permission management on network devices. When enabled, the device sends user login requests to the configured TACACS server, which verifies the user's identity and grants or denies access accordingly.

TACACS Parameter

Tacacs Enable

☒ Enable

Server Address

Server Port

49

Tacacs Key

Device Behavior Upon Tacacs Timeout

Verify Access Locally ▾

Figure 4.16- 10 TACACS Parameter

Explanation of TACACS Parameters:

Tacacs Enable	Enable Tacacs
----------------------	---------------

Server Address	Address of the TACACS server, used as the destination for device authentication requests.
Server Port	Communication port; the default TACACS protocol port is 49, which can be adjusted according to server settings.
Tacacs Key	A pre-shared secret between the device and TACACS server, used for packet encryption and authentication.
Device Behavior Upon Timeout	Handling after TACACS authentication timeout: - Verify access locally: If verification of local web login username and password is successful after timeout, login succeeds. - Deny access: All logins are denied after TACACS authentication timeout.

4.16.11 WEB Log

After enabling WEB Log, access and operation logs generated through the Web management interface will be recorded in log files. The log file size can be configured, and the files can be downloaded directly from the same page.

WEB Log Parameter

WEB Log Enable

☒ Enable

WEB Log File Size

1MB

Save

Download

Figure 4.16- 11 WEB Log

4.17 Security

4.17.1 WEB ACL

ACL (Access Control List) for WEB is used to configure IP addresses (users) that are allowed to access the WEB page of the gateway. The IP address list can't be null once ACL is enabled.

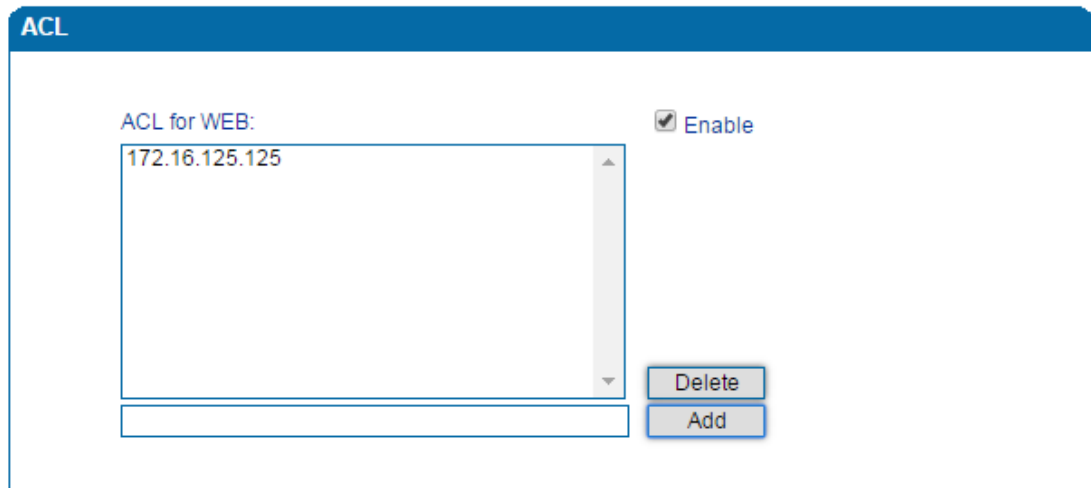


Figure 4.17- 1 ACL for WEB

4.17.2 Telnet ACL

ACL (Access Control List) for WEB is used to configure IP addresses (users) that are allowed to access the Telnet page of the gateway. The IP address list can't be null once ACL is enabled.

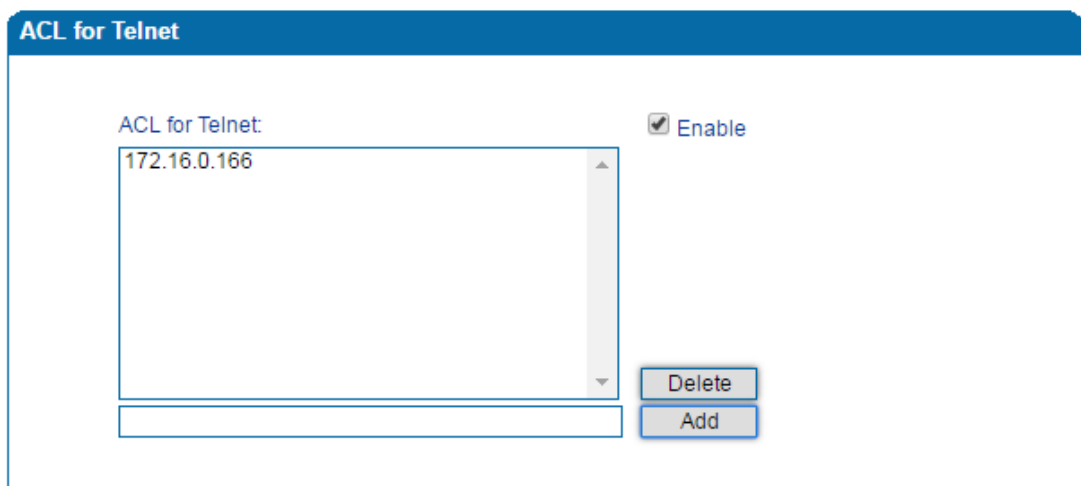


Figure 4.17- 2 ACL for Telnet

4.17.3 Device ACL

Add a packet-filtering rule on the device to allow or block specific traffic reaching the gateway or passing through it. This is typically used to protect device services and control management or data-plane access.

Device ACL - Add

Index

31

▼

Description

Enable

☒

Action

Drop

▼

Source IP

Source Port

Protocol

TCP

▼

Local Port

Device ACL

	Index	Description	Action	Status	Source IP	Source Port	Protocol	Local Port
☐	6	us12	Allow	Enable	--	--	TCP	8080
☐	12	test123	Allow	Enable	172.23.11.222	--	TCP	--
☐	19	us	Allow	Enable	--	5060	UDP	--
☐	23	test234	Drop	Enable	2020:18::23	23006	TCP	--
☐	30	us12ww	Drop	Disable	172.30.33.182	--	UDP	50060
☐	31	test	Drop	Enable	172.23.11.22	5088	TCP	5062

Total: 6 Entry Page 1 ▼

Figure 4.17- 3 ACL for Device

Explanation of Device ACL Parameters:

Index	Index of this device acl rule
Description	Description of this device acl rule
Enable	Whether to enable this device acl rule
Action	What to do when a packet matches the rule. Typical values: Drop or Allow Drop: silently discard matching packets. Allow: permit matching packets.
Source IP	Source IP address of traffic used in matching rules
Source Port	Source port or port range used by the sender
Protocol	Protocol Types: TCP, UDP
Local Port	Local (destination) port or port range.

4.17.4 Firewall-Input Rule

This interface is used to configure the device's Firewall-Input Rule. The page provides multiple types of Access Control List (ACL) settings to control different kinds of traffic entering the device (for example, DHCP, DDOS, SPI, MAC, etc.), and allows specific rules to be enabled, added, modified, or deleted.

Firewall-Input Rule

DDOS ACL

☐ Enable

DHCP ACL

☐ Enable

Index	Description	Source MAC	Status
---	---	---	---

Add

Mod

Del

SPI ACL

☐ Enable

Index	Description	Local Port	Limit Number	Status
---	---	---	---	---

Add

Mod

Del

MAC ACL

☐ Enable

Index	Description	Source MAC	Source IP	Status
---	---	---	---	---

Add

Mod

Del

Note:

1. It is recommended to add common ports such as WEB/SSH before enabling SPI ACL to avoid inaccessibility.
2. It is recommended to add common local MAC addresses before enabling MAC ACL to avoid inaccessibility.

Figure 4.17- 4 Firewall-Input Rule

DDoS Protection

Select whether to enable protection rules against Distributed Denial of Service (DDoS) attacks. When checked DDOS ACL, the device activates the DDoS ACL rules to match and block incoming traffic; if unchecked DDOS ACL, this protection is disabled.

Firewall-Input Rule

DDOS ACL

☒ Enable

DHCP Flood Protection

On the **Security->Firewall-Input Rule** page, configure the DHCP ACL by first adding a rule. You can set the sequence index, description, source MAC address, and enable status.

DHCP ACL - Add

Index

31

Description

Source MAC Address

Enable

☒

Then enable the DHCP ACL, once enabled:

(1) Only allow registered devices with specific MAC addresses to obtain DHCP addresses and limit the number of DHCP requests per second, blocking all other requests;

(2) Discard DHCP packets with abnormal Option fields.

DHCP ACL ☒ Enable

	Index	Description	Source MAC	Status
☐	9	iphone	f8:a0:3d:67:57:08	Enable
☐	24	test12	01:23:45:67:89:12	Disable
☐	31	test	01:23:45:67:89:0B	Enable

MAC Spoofing Protection

On the **Security -> Firewall-Input Rule** page under MAC ACL configuration, first add a new rule where you can set the sequence index, description, source MAC address, source IP, and enable status.

MAC ACL - Add

Index: 28

Description:

Source MAC Address:

Source IP:

Enable: ☒

Then enable the MAC ACL, once enabled:

(1) Only the specified MAC address and source IP are allowed to communicate through the eth0 interface;

(2) Abnormal state packets are dropped.

MAC ACL ☒ Enable

	Index	Description	Source MAC	Source IP	Status
☐	4	mac	60:03:08:97:82:be	172.23.1.185	Enable
☐	29	test	01:23:45:67:89:11	2020:18::23	Disable
☐	30	test	01:23:45:67:89:01	2020:18::23	Enable
☐	31	test	01:23:45:67:89:0A	172.23.1122	Enable

Connection State Detection (Stateful inspection / SPI)

On the **Security->Firewall-Input Rule** page, configure the SPI ACL by first adding a new rule. You can set the sequence index, description, local port, limit number per minute, and enable status. Then enable the SPI ACL.

SPI ACL - Add

Index

Description

Local Port

Limit Number Per Minute

Enable
☒

Then enable the SPI ACL, once enabled:

- (1) Only connections on the specified local ports are allowed, with the connection rate not exceeding the set limit per minute (0 means no limit).
- (2) Packets from established connections are permitted.
- (3) Connections with invalid states are dropped.

SPI ACL
☒ Enable

	Index	Description	Local Port	Limit Number	Status
☐	0	web_https	443	0	Enable
☐	1	ssh_1	22	0	Enable
☐	11	test123w	8080	60	Enable
☐	30	sip	5062	120	Enable

4.17.5 Passwords

On the following interface user can configure or modify the username and password for access the WEB interface and the Telnet interface.

Password Modification	
Web Config	
Old Web Username	admin
Old Web Password	
New Web Username	
New Web Password	
Confirm Web Password	
Telnet Config	
Old Telnet Username	admin
Old Telnet Password	
New Telnet Username	
New Telnet Password	
Confirm Telnet Password	

Figure 4.17- 5 Password Modification

Note:

Default username and password: Web — admin / admin@123#; Telnet — admin / admin. It is advised to modify them for security consideration.

4.17.6 Encrypt

When the DAG1000-4S device is registered to a VOS softswitch, you can encrypt SIP and RTP for the VOS softswitch.

Encryption Configuration	
SIP Encrypt	Enable
RTP Encrypt	RTP
Encrypt Mode	VOS RC4

Figure 4.17- 6 Encrypt

4.17.7 Certificate Manage

Certificate manage interface allows users to upload custom web HTTPS certificates and SIP certificates.

SIP CA certificates and SIP client certificates are key components for securing VoIP communications based on the SIP protocol, essential for implementing TLS/SRTP encryption and mutual authentication.

Web HTTPS certificates are digital certificates based on the SSL/TLS protocol, used to verify website identity and encrypt communication between browsers and servers.

SIP Client Certificate				
Awarded	Issuer	Start Time	End Time	
--	---	---	---	---

SIP CA Certificate					
Index	Awarded	Issuer	Start Time	End Time	☐
0	--	---	---	---	---
1	--	---	---	---	---
2	--	---	---	---	---
3	--	---	---	---	---
4	--	---	---	---	---

Delete

WEB Https Certificate				
Awarded	Issuer	Start Time	End Time	
dinstar	dinstar.com	2018-09-10 09:52:0	2028-09-07 09:52:0	---

Certificate Upload

File Type

SIP CA Certificate ▼

Upload SIP CA Certificate.

SIP CA Certificate

选择文件 未选择文件

Upload

Note:1.Upload file must be certificate format.
 2.Please restart the device to take effect.
 3.SIP CA Certificate cannot be uploaded repeatedly.

Certificate Configuration

Verification certificate

☐ Enable

Figure 4.17- 7 Certificate Manage

4.18 Tools

4.18.1 Firmware upload

On the **Tools -> Firmware Upload** page, you can upload a new firmware version from a local folder.

Figure 4.18- 1 Firmware Upload

Steps of Firmware Uploading:

Step 1 Check the current firmware version on the **System Information page**

Current Software Version DAG1000-4S 2.83.13.05 PCB 20 LOGIC 0 BIOS 1, 2025-05-14 17:28:17
 Backup Software Version DAG1000-4S 2.83.13.05 PCB 20 LOGIC 0 BIOS 1, 2025-05-14 17:28:17
 DSP Version ARM_32_13 Jan 13 2022 17:39:22
 U-BOOT Version 25
 Kernel Version 30
 Root FS Version 25
 FS Version 24
 Hint Language Chinese

Step 2 Prepare firmware package. The most important is that the package must match with the existing version. Package version consists of the following parts:

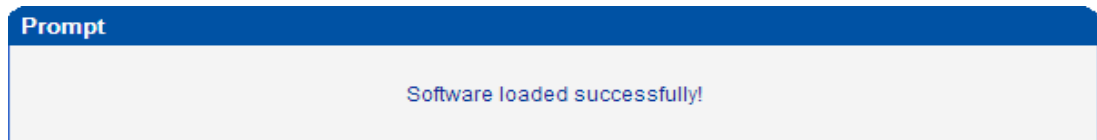
2.83.xx.xx

01/02 is vendor name

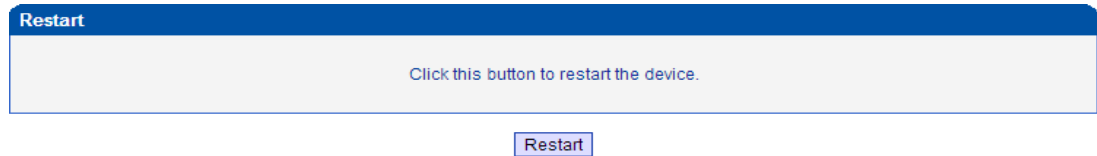
83 is hardware version, xx.xx is version number

Step 3 Upload firmware, select the package from specific folder on the computer and click **Upload** button.

Step 4 Keep waiting until it prompts 'Software loaded successfully!'



Step 5 Reboot gateway. Refer to web page **Tools-> Device Restart**



4.18.2 Data Backup

On the **Tools -> Data Backup** page, you can download and backup configuration data, device status and summary messages on local computer.

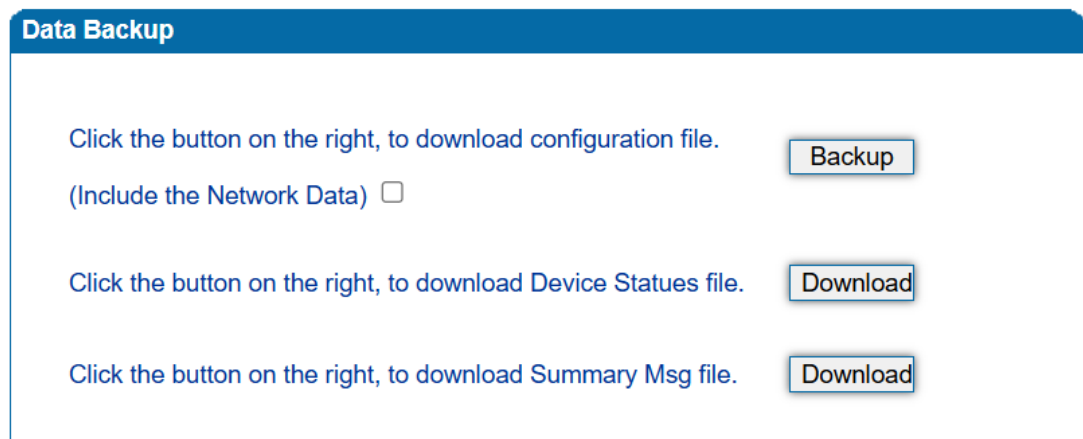


Figure 4.18- 2 Data Backup

4.18.3 Data Restore

On the **Tools -> Data Restore** page, you can restore configuration data through uploading a data file from local computer. The restored configurations will take effect after the device is restarted.

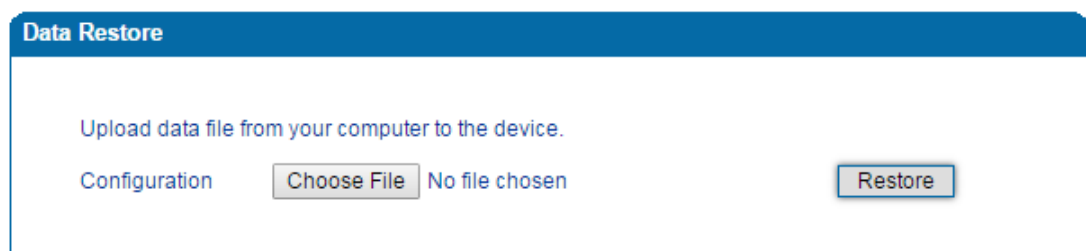


Figure 4.18- 3 Data Restore

4.18.4 Outward Test

Outward test enable user to diagnose the physical phone lines which follow GR909 standards. To startoutward test, select the FXS ports to be tested and click 'start'. Testing costs a few minutes.

Outward Test						
Port	Enable	Loop Open	H.F. DC Voltage(V)	H.F. AC Voltage(mV)	Tip/Ring Short	Result
1	☐					
2	☐					
3	☐					
4	☐					
Options ☐ Test All Ports						

Figure 4.18- 4 Outward Test

Test results:

OK: the analog phone set and phone line are working well

FAIL: analog phone doesn't connect to FXS port or there's something wrong in phone set

4.18.5 Ping Test

Ping is used to examine whether a network works normally through sending test packets and calculating response time.

Instructions for using Ping:

- 1) Enter the IP address or domain name of a network, a website or a device in the input box of Ping, and then click **Start**.
- 2) If related messages are received, it means the network works normally; otherwise, the network is not connected or is connected faultily.

Ping Test

Destination

www.bing.com

Number of Ping(1-100)

4

Packet Size(56-1024 bytes)

56

Start

Stop

Information

Pinging www.bing.com[Resolve: 13.107.21.200] with 56 bytes of data:
Reply seq=0 from 13.107.21.200: bytes=56 time=60ms TTL=115
Reply seq=1 from 13.107.21.200: bytes=56 time=60ms TTL=115
Reply seq=2 from 13.107.21.200: bytes=56 time=70ms TTL=115
Reply seq=3 from 13.107.21.200: bytes=56 time=50ms TTL=115

Ping statistics for 13.107.21.200
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
RTT Minimum = 50ms, Maximum = 70ms, Average = 60ms

Figure 4.18- 5 Ping Test

4.18.6 Tracert Test

Tracert is short for traceroute, used to track a route from one IP address to another..

Instruction for using Traceroute:

- 1) Enter the IP address or domain name of a destination device in the input box of Traceroute, and then click Start.

Destination: the IP address or domain name of a destination device that needs to be tracked.

Max Hops: the maximum hops for searching the above IP address or domain name. For example, if 'max hops' is set as 30, and the configured IP address or domain name cannot be reached within 30 hops, it's thought that the IP address or domain name cannot be searched.

- 2) View the route information from the returned message.

Tracert Test

Destination

Max Hops(1-255)

Start

Stop

Information

Tracing route to www.google.com[Resolve: 173.194.127.240] over a maximum of 30 hops:

```

1  10 ms  172.16.1.1
2  1 ms   113.106.38.109
3  *      Request timed out.
4  10 ms  121.34.242.234
5  10 ms  202.97.33.242
6  10 ms  202.97.60.50
7  *      Request timed out.
8  *      Request timed out.

```

Figure 4.18- 6 Tracert Test

4.18.7 Network Capture

Network capture is a very important diagnostic tool for maintenance. It can be used to capture data packages of the available network ports.

PCM Capture:

PCM capture helps to analysis voice stream between analog phone and DSP chipset.

Network Capture

Type

☒ Network package
☒ PCM
☐ Syslog
☐ DSP

Port

Port 1

Start

Stop

- Click “Start” to enable PCM capture
- Dialing out through the device, start talking a short while then hang up the call.
- Click ‘Stop’ to disable network capture
- Save the file to local computer

The captured package is named to ‘capture(x).pcap’, among which x is the serial number of the capturing and will be added 1 in next time. The sample of PCM capture as below:

No.	Time	Source	Destination	Protocol	Length	Info	Ch: 0xFFFF, Seq: 8 (From Host)
1	0.000000	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x0021	
2	0.000131	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
3	0.000245	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	44	--> 0x0021	Ch: 0xFFFF, Seq: 11 (From Host)
4	1.320893	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x0e00	Ch: 0x0003, Seq: 0 (From Host)
5	1.321022	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
6	1.321129	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	30	--> 0x0e00	Ch: 0x0003, Seq: 1 (From Host)
7	1.329890	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x0e01	Ch: 0x0003, Seq: 1 (From Host)
8	1.330010	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
9	1.330093	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	30	--> 0x0e01	Ch: 0x0003, Seq: 2 (From Host)
10	1.330472	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x0802	Ch: 0x0003, Seq: 2 (From Host)
11	1.330566	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
12	1.330639	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	30	--> 0x0802	Ch: 0x0003, Seq: 3 (From Host)
13	1.330820	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x0803	Ch: 0x0003, Seq: 3 (From Host)
14	1.330903	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
15	1.330989	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	30	--> 0x0803	Ch: 0x0003, Seq: 4 (From Host)
16	1.337791	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x9010	Ch: 0x0003, Seq: 4 (From Host)
17	1.337996	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
18	1.338033	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	30	--> 0x9010	Ch: 0x0003, Seq: 5 (To Host)
19	1.338369	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x9000	Ch: 0x0003, Seq: 5 (From Host)
20	1.338460	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
21	1.338564	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	30	--> 0x9000	Ch: 0x0003, Seq: 6 (To Host)
22	1.343521	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x8084	Ch: 0x0003, Seq: 6 (From Host)
23	1.343627	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
24	1.343725	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	30	--> 0x8084	Ch: 0x0003, Seq: 7 (To Host)
25	1.344060	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x8001	Ch: 0x0003, Seq: 7 (From Host)

Syslog Capture:

Syslog capture is another way to obtain syslog which the same as remote syslog server and filelog. The capture file is save as pcap format so that it can be opened in some of capture software like Wireshark, Ethereal software etc.

Network Capture

Type
☒ Network package
☐ PCM
☒ Syslog
☐ DSP

Start
Stop

- Click "Start" to enable syslog capture
- Dialing out through gateway, start talking a short while then hangup the call.
- Click "Stop" to disable syslog capture
- Save the capture to local computer

The capture package is named to 'capture(x).pcap', x is serial number of capture and will be added 1 in next time. The sample of syslog capture as below:

No.	Time	Source	Destination	Protocol	Length	Info	
1	0.000000	172.16.222.22	1.1.1.1	Syslog	172	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 0>	[DEBUG] ----> to 172.16.222.22/5060 crypt:FALSE Phone
2	0.000344	172.16.222.22	1.1.1.1	Syslog	520	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 1>	[DEBUG] OPTIONS sip:heartbeat@172.16.222.22 SIP/2.0\r\n
3	0.003432	172.16.222.22	1.1.1.1	Syslog	595	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 2>	[DEBUG] <----- message from 172.16.222.22/5060, crypt
4	0.013750	172.16.222.22	1.1.1.1	Syslog	176	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 3>	[DEBUG] <----- from 172.16.222.22/5060, crypt:FALSE, PHC
5	0.014036	172.16.222.22	1.1.1.1	Syslog	520	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 4>	[DEBUG] OPTIONS sip:heartbeat@172.16.222.22 SIP/2.0\r\n
6	0.014512	172.16.222.22	1.1.1.1	Syslog	172	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 5>	[DEBUG] <----- to 172.16.222.22/5060 crypt:FALSE Phone
7	0.014806	172.16.222.22	1.1.1.1	Syslog	587	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 6>	[DEBUG] SIP/2.0 200 OK\r\nvia: SIP/2.0/UDP 172.16.222.22
8	0.028396	172.16.222.22	1.1.1.1	Syslog	662	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 7>	[DEBUG] <----- message from 172.16.222.22/5060, crypt
9	0.028759	172.16.222.22	1.1.1.1	Syslog	176	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 8>	[DEBUG] <----- from 172.16.222.22/5060, crypt:FALSE, PHC
10	0.029052	172.16.222.22	1.1.1.1	Syslog	587	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 9>	[DEBUG] SIP/2.0 200 OK\r\nvia: SIP/2.0/UDP 172.16.222.22
11	0.030017	172.16.222.22	1.1.1.1	Syslog	233	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 10>	[DEBUG] sip->app: msgtype:STP_SERVER_CONN \r\n cal
12	0.331167	172.16.222.22	1.1.1.1	Syslog	983	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 11>	[DEBUG] <----- message from 172.16.222.22/5060, cryp
13	0.331498	172.16.222.22	1.1.1.1	Syslog	177	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 12>	[DEBUG] <----- from 172.16.222.22/5060, crypt:FALSE, PHC
14	0.331959	172.16.222.22	1.1.1.1	Syslog	907	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 13>	[DEBUG] INVITE sip:100860172.16.222.22/5060 SIP/2.0\r\n
15	0.332307	172.16.222.22	1.1.1.1	Syslog	122	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 14>	[DEBUG] get route entry 31\r\n
16	0.332584	172.16.222.22	1.1.1.1	Syslog	111	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 15>	[DEBUG] port:3\r\n
17	0.332848	172.16.222.22	1.1.1.1	Syslog	124	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 16>	[DEBUG] get route, to port:3\r\n
18	0.333315	172.16.222.22	1.1.1.1	Syslog	526	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 17>	[DEBUG] sip->app: localIndex:69, msgtype:STP_CALL_INV
19	0.333603	172.16.222.22	1.1.1.1	Syslog	173	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 18>	[DEBUG] <----- to 172.16.222.22/5060 crypt:FALSE, PHC
20	0.333877	172.16.222.22	1.1.1.1	Syslog	386	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 19>	[DEBUG] SIP/2.0 100 Trying\r\nvia: SIP/2.0/UDP 172.16.222.22
21	0.346887	172.16.222.22	1.1.1.1	Syslog	131	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 20>	[DEBUG] RTP: alg:0, pkt:20, band:-1\r\n
22	0.347453	172.16.222.22	1.1.1.1	Syslog	120	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 21>	[DEBUG] dial tick:102433\r\n
23	7.232839	172.16.222.22	1.1.1.1	Syslog	533	USER.DEBUG: Jul 23 06:52:12 172.16.222.22 mpe_sip: < 22>	[DEBUG] <----- message from 172.16.222.22/5060, cryp
24	7.233513	172.16.222.22	1.1.1.1	Syslog	177	USER.DEBUG: Jul 23 06:52:12 172.16.222.22 mpe_sip: < 23>	[DEBUG] <----- from 172.16.222.22/5060, crypt:FALSE, PHC
25	7.233959	172.16.222.22	1.1.1.1	Syslog	457	USER.DEBUG: Jul 23 06:52:12 172.16.222.22 mpe_sip: < 24>	[DEBUG] CANCEL sip:100860172.16.222.22/5060 SIP/2.0\r\n
26	7.234596	172.16.222.22	1.1.1.1	Syslog	287	USER.DEBUG: Jul 23 06:52:12 172.16.222.22 mpe_sip: < 25>	[DEBUG] sip->app: LocalIndex:69, msgtype:STP_CALL_BYE

DSP Capture:

DSP capture helps to analysis voice stream inside DSP chipset. The DSP chipset will handle RTP from IP networks as well as voice stream from analog phone.

Network Capture

Type

☒ Network package
 ☐ PCM
 ☐ Syslog
 ☒ DSP

Start

Stop

- Click "Start" to enable syslog capture
- Dialing out through gateway, start talking a short while then hangup the call.
- Click 'Stop' to disable syslog capture
- Save the capture to local computer

The capture is named to 'capture(x).pcap', x is serial number of capture and will be added 1 in next time. The sample of RTP capture as below:

No.	Time	Source	Destination	Protocol	Length	Info	
1	0.000000	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x0021	Ch: 0xFFFF, Seq: 2 (From Host)
2	0.007246	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
3	0.007260	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	44	--> 0x0021	Ch: 0xFFFF, Seq: 5 (From Host)
4	2.994581	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x0021	Ch: 0xFFFF, Seq: 3 (From Host)
5	2.997308	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
6	2.997316	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	44	--> 0x0021	Ch: 0xFFFF, Seq: 6 (From Host)
7	5.992790	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x0021	Ch: 0xFFFF, Seq: 4 (From Host)
8	5.997282	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
9	5.997290	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	44	--> 0x0021	Ch: 0xFFFF, Seq: 7 (From Host)
10	7.691428	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x9010	Ch: 0x0003, Seq: 3 (From Host)
11	7.691552	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
12	7.691715	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	30	--> 0x9010	Ch: 0x0003, Seq: 1 (To Host)
13	7.701379	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x9000	Ch: 0x0003, Seq: 4 (From Host)
14	7.701494	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
15	7.701622	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	30	--> 0x9000	Ch: 0x0003, Seq: 2 (To Host)
16	7.709662	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x8084	Ch: 0x0003, Seq: 5 (From Host)
17	7.709798	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
18	7.709902	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	30	--> 0x8084	Ch: 0x0003, Seq: 3 (To Host)
19	7.710238	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x8001	Ch: 0x0003, Seq: 6 (From Host)
20	7.710328	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II [Malformed Packet]	
21	7.710496	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	30	--> 0x8001	Ch: 0x0003, Seq: 4 (To Host)

4.18.8 Factory Reset

Click 'Apply' to restore configurations of the device to the factory default settings.

Default Set

Click the button below to reset to factory default settings.

Apply

Figure 4.18- 7 Reset Device to Factory Default Setting

4.18.9 Device Restart

After saving all the configurations or changes to the equipment, user can restart the DAG1000-4S gateway for the changes to take effect.

Restart

Click the button below to restart the device.

Restart

Figure 4.18- 8 Restart Gateway

5 Trouble Shooting

(1) Cannot access the GUI of the gateway?

- a. Check the device RUN indicator status. If the RUN indicator remains constantly on or off, the device may be malfunctioning. Please contact online technical support to confirm.
- b. Connect the device's network port directly to a PC with an Ethernet cable and see if the PC recognizes the network adapter. If the PC does not detect the network adapter or the device's network port indicator are off, try a different device network port, a different cable, or another PC. If the network port is recognized, assign the PC an IP address in the same subnet as the gateway device, then try to ping the device IP.
- c. Verify the web port. The default port is 80 (browsers omit: 80). If the device GUI port was changed, enter the correct port in the browser (for example: <https://<IP>:<port>>).
- d. If you cannot determine the device IP or web port, try restoring the device to the default network configuration and default username/password by pressing the RST button for 3-6 seconds or dialing *165*000000# from a phone; or restore factory configuration by pressing RST for 7-9 seconds or dialing *166*000000# from a phone. Then set your PC to an address in the gateway subnet such as 192.168.11.XXX.

(2) Forget the IP address of the analog gateway

- a. Dial *158# to query the IP address of LAN port of the gateway;
- b. Pressing the RST button for 3-6 seconds or dial *165*000000# from a phone to restore the device's default network configuration and default login username/password.
- c. Pressing RST for 7-9 seconds or dial *166*000000# from a phone to restore factory settings.

(3) Forget username and password of the analog gateway

- a. Pressing the RST button for 3-6 seconds or dial *165*000000# from a phone to restore the device's default network configuration and default login username/password.
- b. Pressing RST for 7-9 seconds or dial *166*000000# from a phone to restore factory settings.

(4) Port/account registration failed.

- a. Open the device web GUI, click “Tools -> Ping Test” and ping the registration server address to check network connectivity between both ends. If ping fails, the network is not reachable. Check the device's network mode, when in router mode you must connect the WAN port. If the device connections and network mode are correct, ask your network technician to investigate routing, gateway, firewall, NAT, etc.
- b. Verify the data provided by the server, including SIP server address and SIP port, SIP Authenticate account and password (When entering the SIP account and password, ensure there are no extra spaces).

6 Glossary

Abbr.	Full Name
DNS	Domain Name System
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
RTP	Real Time Protocol
PPPOE	point-to-point protocol over Ethernet
VLAN	Virtual Local Area Network
ARP	Address Resolution Protocol
CID	Caller Identity
DND	Do NOT Disturb
DTMF	Dual Tone Multi Frequency
NTP	Network Time Protocol
DMZ	Demilitarized Zone
STUN	Simple Traversal of UDP over NAT
PSTN	Public Switched Telephone Network
IMS	IP Multimedia Subsystem
ACL	Access rule list
SNMP	Simple Network Management Protocol
FXS	Foreign Exchange Station

Shenzhen Dinstar Co., Ltd.

Address: Floor 18, Building 7A, Vanke Cloud City Phase 1, Xingke 1st Street, Xili Sub-district, Nanshan District, Shenzhen.